‘ASSAULTING THE INVIOLABILITY OF CITIZENS PRIVATE LIVES IN THE NAME OF THE ANTI-CYBERCRIME LAW AND THE BREACH OF COMMUNICATIONS AND INTERNET USERS' PERSONAL PRIVACY

ANHRI

Assaulting the inviolability of citizens' private lives in the name of the law...

Anti-Cybercrime Law and the breach of communications and internet users' personal privacy

Introduction

The conceptual definitions of individual freedoms and rights were historically established to confront the state's encroachment on citizens' rights and freedoms. Consequently, the concept that citizens are entitled to enjoy non-derogable rights has emerged after a long battle to curtail the state's unlimited powers.

Personal space, which is bounded by the walls of every person's home and extends in particular to his personal communication with others, has been the focus of the various legislations and laws that sought to protect citizens from any interference in their personal lives. Such laws have been subject to amendments all along; owing to the massive breakthrough that personal data storage technologies have undergone. This development is always accompanied with a greater risk of exposing such data and communication to violation by external bodies on top of which state authorities.

In light of the substantial development of electronic means of communication especially the Internet and its various applications that are no longer limited to personal computers, but expanded to include smartphones, which allow us to save or store most of our data electronically and to exchange it with different people and destinations all the time using network connectivity, it has become necessary to protect our privacy in order to preserve this amount of data and communications which may be used to harm us in one way or another. On the other hand, state bodies may resort, under certain circumstances, to access personal data and correspondence to collect evidence that will help in convicting the perpetrators of various crimes or in disclosing plans for criminal acts targeting national security, especially terrorist crimes. Therefore, enacting laws that protect the privacy of saving data and private correspondence should take into account the cases in which the security services can access such data, as well as the safeguards that would prevent- under judicial orders- any violation of the inviolability of such personal information and communications of citizens, and hence endangering their security and safety.

This paper:

This paper briefly outlines the articles of Law No. 175 of 2018 Regarding Anti-Cyber and Information Technology Crimes; related to the protection of citizens' personal data and communications by enabling the security services- or what the law called 'the national security agencies'- to have access to this information.

The paper aims to:

1- Informing citizens how this law provides for the protection of their personal data.

2- Indicating the extent to which this law ensures the requisite balance between requirements of public interest and the protection of citizens' right to privacy and the consequent protection of their security and safety.

The legal and constitutional framework:

The Universal Declaration of Human Rights states that "Everyone has the right to life, liberty and security of person and that no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence". It also provides that "Everyone has the right to the protection of the law against such interference or attacks", while recognizing the right to a social and international order in which the rights and freedoms set forth in this Declaration can be fully realized.

Additionally, the International Covenant on Civil and Political Rights, which has entered into force in Egypt since 1981, confirms- in Article 17 thereof- the inadmissibility of interference neither in one's private life nor in the affairs of his family, home, and correspondence.

Article (17) of the International Covenant on Civil and Political Rights states that:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.

Also, the Egyptian Constitution provides for the inviolability of private life, postal, telegraphic and electronic correspondences, telephone calls, and other means of communication, and prohibits confiscating, revealing or monitoring them except by virtue of a reasoned judicial order, for a definite period, and in cases specified by Law (Articles 57 and 58).

The Constitution also states that every person has the right to a secure life and that the state shall provide security and reassurance for citizens, and all those residing within its territory.

Law No. 175 and privacy

First: Endangering citizens' privacy in general

Article (2) of the Law No. 175/2018 Regarding Anti-Cyber and Information Technology Crimes requires "service providers", i.e. telecommunications/internet companies, to do the following:

1- Retain and store the information system data or any other means of information technology for a default period of 180 days. This data includes the following:

(A) Personal identifiers (information that identifies the service's user)
(B) Metadata (data related to the content of the information system)
(C) Data related to communication traffic.
(D) Data related to communication peripherals.
(E) Any other data specified by the competent authority

This article violates citizens' right to privacy for the following reasons:

1- Service providers are obligated to retain and store data that may exceed what they need in order to complete their work efficiently, noting that this data is not related with, nor owned whatsoever by, telecommunication or internet companies; rather it is fully owned by the service's users.
2- Service providers are obligated to keep this data for a long period of time, and the longer this period is, the more this data is subject to interference, piracy and illegal or commercial access, which would lead to violation of citizens' privacy in a way

that makes it difficult to determine the violator; whether he is among the service provider's information system or outside it.

3- This article gives the administrative, non-legislative or judicial authorities the right to determine additional types of data that deems unknown, unspecified and unlimited by obliging service providers to retain and store them. This constitutes a gross breach of the service's user's right to information when the service provider is entitled to keep and store data in advance and in detail.

Second: The powers granted to the national security agencies

Although the law obligates telecommunications and internet companies (service providers) to maintain the privacy and confidentiality of the data being stored by forcing them not to reveal it except by virtue of a reasoned judicial order, the Cybercrime Law grants the "national security" agencies- which it defines as: the presidency of the republic, the Ministry of Defense, the Ministry of Interior, the General Intelligence Service, the Administrative Control Authority (ACA)- the right to benefit from this reasoned judicial order in the following way:

- The competent authorities may access, seize, attach, or trace information, data, or information systems in any medium or electronic program or computer.

- They may search and access the computer's programs databases and other information system as part of the powers granted to them to achieve their goal.

- The authorities may order service providers to turn over any information related to users' activities or to an information system or technical device that is under his control, as well as the data of the users of his service and the traffic of communications that took place on that system or technical device.

The aforementioned articles are fundamentally flawed due to the following reasons:

1- Inconsistency: Some articles require a judicial order to access the data, while others grant discretionary power to an unidentified investigative body, and other articles gives powers to the "national security services" themselves under no requirements (whether obtaining a judicial order or an investigative body).

2- The law doesn’t specify any regulations with regard to the reasons or circumstances under which a judicial order could be issued to access the user's data. It also doesn’t specify what sort of data that the judicial order may cover.

3- The law grants an unknown party the right to file an appeal against the judicial order, without requiring notifying the concerned person (the service's user) of the matter. It also does not specify a time period to lodge an appeal before the decision is actually implemented. The law also does not stipulate any means of compensation in case the reasons for requesting access to the data are insufficient or incorrect causing harm to the owner of the data or endangering his safety.

4- The most dangerous point is that the aforementioned articles of the law allow national security agencies to access all the information system's data and don’t confine the matter to certain users to whom the court order may relate (when it is required to obtain a judicial order), making the data of all information system's users accessible under no legal justification or regulations.

Third: Intimidating service providers

The law makes service providers be held criminally responsible in the following cases: when any of them refrained from turning over their data or information, or letting the national security services seize, attach, or trace information, data, or information systems in any medium or electronic program or computer, or search and access the computer's programs databases and other information systems. Service providers hence will be punished by imprisonment for a period of no less than six months and a fine of no less than EGP 20,000 and no more than EGP 100,000, or either of these two penalties.

Conclusion and recommendations

The Law No. 175 of 2018 utterly disregards the constitutional and human rights guarantees of privacy and the inviolability of private life. In practice, it renders the electronic data of users of the Internet and communication services completely available and accessible for national security agencies, under no judicial control or clear regulation, and without providing genuine means of grievance to avoid the harm resulting from such violation of privacy or even providing a compensation for the harm if it occurs.

Therefore, this paper recommends amending Law 175 of 2018 so that its articles would fully comply with the Egyptian Constitution and the international human rights charters and covenants that Egypt ratified. The amendments should include the following:

1- Not to oblige or allow service providers to keep or store data that goes beyond that needed for performing their duties and for the period necessary for them to carry out their job. In other words, the law should explicitly determine the sort of data that is needed to be examined or disclosed, and confine the need to disclose the data to judicial authorities only, while arranging penalties in case the service provider retains data that violates the consent that it obtained from its users.

2- In case investigations into a specific crime necessitate having access to the data of a user of telecommunications and Internet services, or to retain the data for a specific period, the law should stipulate that regulations under which such a request can be met when submitting it to an independent judicial authority. Such regulations can include: mentioning the person (s) whose data is required to be accessed and the reasons that would justify this request, in addition to identifying the sort of data that is required to be accessed or disclosed, and in case the request is related to storing the data for a specific period of time (which is analogous to placing a person under police surveillance), it is required to determine this period and the reasons behind the request to store the data.

3- The law should not stipulate that service providers are required to grant any governmental or non-governmental entity full access to its information systems, under any circumstance. This can rather be limited to the data that is specified by a reasoned judicial order and for a specific period of time.