TECHNOLOGY & LAW COMMUNITY

The Right to Privacy in Egyptian Laws.. Legislative Obstacles and Unfinished Steps

Masaar-Technology and Law Community

June 2021

Masaar.net

Creative Commons: Attribution 4.0 International (CC BY 4.0)

Contents

Introduction

Egypt has passed these recent years through successive legislative developments aiming, largely, to attempt establishing organizational and procedural rules for the technological developments and the use of information technology by individuals and companies.

Such legislative developments come under the notion that technological development requires laws that enhance and protect the rights of individuals in their private lives and personal data, and guarantees redress for victims of violations of these rights.

The Personal Data Protection Law No. 151 of 2020 is among the legislations recently issued in this context. However, the rules established by this law are not yet effective for a variety of reasons that will explain this paper.

The recently passed legislation intended to protect the right to privacy detached from reality, where these legislations did not take into account the urgent need to review a large number of laws, decisions of laws, and other administrative decisions which constitutes a large part of the legislative structure in Egypt that impede the exercise of this right, and limit the effectiveness of the constitutional protection guaranteed to it.

This conflict arises between these new laws from one side and the entire legislative structure on the other, in light of the increasing importance of the right to privacy in the time of technological development that has increased the capabilities of governments and companies to threaten the privacy of individuals, either through the use of mass surveillance technologies and the ability to intercept and collect data, or through inspection procedures and other practices that violate the privacy of users.

The right to privacy is one of those rights that reveal the conditions of rights and freedoms in the society in general in terms of its influence on and connection with many other rights, such as: freedom of expression, the right to organize and peaceful assembly, and the right of access to and exchange of information.

This connection has been evident with the spread of COVID-19, and the impact of the way governments and companies handle the pandemic and their plans to face it on many rights and freedoms.

Meanwhile, alongside the development of daily practices carried out by successive governments and service providers which violate the right to privacy, some say that most of these practices take place outside the framework of the law, and that they are procedures that lack the legitimacy necessary to rely on as legal procedures. However, practices associated with violating the right to privacy, which this paper will attempt to address, are not outside the law, but are rather reinforced by the law itself through the adoption of unclear vague texts by the legislator which adopt a narrow concept of the right to privacy; a right emptied of its content.

So, this study aims to shed some light on some of the common characters and features in a number of legislations that constitute major obstacles and have be reviewed to ensure that the privacy of individuals is protected, and have also to be read in light of the constitutional rules and obligations stipulated in a number of international conventions, that provide a protection umbrella for the privacy of users.

The right to privacy in the Egyptian constitution

The Egyptian constitution addresses the concept of the right to privacy in more than one place, where on one side it reviews the aspects related to the privacy of users in relation to the means of communication, and - through some scattered texts - addresses the guarantees related to the procedures to be followed during the search of individuals and homes, and their relationship to the sanctity of private life together with the related controls and procedures, on the other side, in addition to a special provision regarding the means of compensation and redress for the harm resulting from violating private life.

The Egyptian constitution – issued in 2014 – specified the text of Article 57 to list various forms of protecting the right to privacy in communications

The first paragraph of this text is considered to be an extension of Article 45 of Egypt's permanent constitution issued in 1971, which has been enforced for nearly 40 years.

However, the text of Article 57 of the Egyptian Constitution issued in 2014 came as a comprehensive text, referring to the organic link between the protection of private life and its relationship to freedom of communication.

The text of Article 57 of the Egyptian Constitution included, in addition to forms of protecting the right of privacy for users, the right to use public means of communication, as well as determining the rules related to exceptions to this right.

"Private life is inviolable, safeguarded and may not be infringed upon. Telegraph, postal, and electronic correspondence, telephone calls, and other forms of communication are inviolable, their confidentiality is guaranteed and they may only be confiscated, examined or monitored by causal judicial order, for a limited period of time, and in cases specified by the law.

The state shall protect the rights of citizens to use all forms of public means of communication, which may not be arbitrarily disrupted, stopped or withheld from citizens, as regulated by the law."

Article 57: Private life of 2014 Egyptian Constitution

What is evident from the wording of Article 57 of the Egyptian Constitution, is the link between the freedom of communication and the right to privacy of users. However, the text regarding the protection of private life, was categorical, without mentioning the exceptions or the need to refer to the law for regulatory details, which does not allow the parliamentary legislator to intervene to set legislative rules through which restrictions may be put on this right, and that the power of the parliamentary legislator stops at setting legal texts that respect the protection of private life, in implementation of the text of Article 57 of the Constitution.

The text of the article has not included whatever would allow deviations from this rule, except in case of executing judicial orders which were also subject to time controls and justifications that must be clear. Moreover, the text of Article 57 of the Constitution in its second paragraph has included wordings that may allow the parliamentary legislator to stipulate controls related to the regulation of the process of disabling or suspending the means of communication, and has set only one restriction on the parliamentary legislator, so that the suspension or disabling of communications shall not be arbitrary.

The Egyptian constitution also included a reference to the inspection process

and its relationship to the sanctity of private life, as it was mentioned in two different places; the first position is related to the people searches, and the second is home searches.

Personal freedom is a natural right which is safeguarded and cannot be infringed upon. Except in cases of in flagrante delicto, citizens may only be apprehended, searched, arrested, or have their freedoms restricted by a causal judicial warrant necessitated by an investigation.

Article 54: Personal freedom

Homes are inviolable. Except in cases of danger, or if a call for help is made, they may not be entered, searched, monitored or wiretapped except by causal judicial warrant specifying the place, time and purpose thereof. All of the above is to be conducted in cases specified by the law, and in the manner prescribed. Upon entering or searching homes, those inside shall be notified and informed of the warrant issued in this regard.

Article 58: Inviolability of homes

The texts of the Egyptian constitution related to the searches, define the terms and conditions that allow the controlling authorities, to take exceptional measures, such as searches of individuals, searches of homes, surveillance and wiretapping. The text of Article 54 and Article 58 are considered complementary to the text of Article 57 of the Constitution which addresses the privacy of users of the means of communication, for reasons related to the practical reality that relates to the widespread practice of searching individuals and homes, and the consequent examination of electronic devices during the inspection process, and the legal proceedings that may follow.

In addition to texts that protect the right to privacy, the Constitution has included a special provision regarding the inadmissibility of statute of limitations for crimes related to violations of rights and freedoms in general, and crimes that constitute an attack on the private life of citizens in particular.

Any assault on the personal freedoms or sanctity of the life of citizens, along with other general rights and freedoms guaranteed by the Constitution and the law, is a crime with no statute of limitations for both civil and criminal proceedings. The injured party may file a criminal suit directly.

The state guarantees just compensation for those who have been assaulted. The National Council for Human Rights shall inform the prosecutor's office of any violation of these rights, and also possesses the right to enter into an ancillary civil lawsuit on the side of the injured party at its request. This is as specified within the law.

Article 99: Violation of personal freedom

The wording of the text of Article 99 of the current constitution is similar to the wording of Article 57 of the 1971 constitution , however, the current constitution made some amendments to the wording of the article, where the text gives a person who has been harmed as a result of an attack on his private life, the right to file a criminal case directly against the person or entity for which the right to privacy was violated. The text also explicitly gives the right to the possibility of filing adirect lawsuit to those who have been harmed, directly to the court to prove the damage inflicted on them and then the right to compensation for these damages,

without the need to file a complaint with the Public Prosecution that has the power to refer the matter to the court or dispose of the investigation of the incident with custody.

The text has also been further modified allowing the National Council for Human Rights to report to the Public Prosecution any violation of these rights, and to intervene in the civil lawsuit, joining the injured party, at its request.

Incomplete legislative attempts to protect the privacy of the users

Recent legislative developments – related to the adoption of a number of laws related to communication technology – have attempted to set some rules aiming to protect the privacy of users, but most were not completed for a variety reasons.

These attempts began when the law against information technology crimes – known as the Cybercrime Law – was established, where the draft law that was presented by the Egyptian government to Parliament – regarding the Law on Combating Information Technology Crimes – referred to one of the objectives of the bill being; "The protection of personal data and information, from exploiting them against their owners, especially in light of the inadequacy of the traditional criminal texts related to protecting the privacy of individuals and the sanctity of their private lives, in the face of emerging threats and risks from using information technology. "

The objectives – included in the project submitted by the Egyptian government – have been reflected, in the recent phrasing of the Anti-Cyber and Information Technology Crimes Law No. 175 for 2018, therefore,

the legislator singled out a separate chapter dedicated to criminalize various acts of which each constitutes a violation of private life , titled; "crimes related to violations on the sanctity of private life and illegal information content".

---

1 - Article 45 of 1971 Egyptian Constitution: “The law shall protect the inviolability of the private life of citizens. Correspondence, wires, telephone calls and other means of communication shall be inviolable and secret and may not be seized or put under surveillance except by judicial warrant and for a limited period according to the provisions of the law.”

2 - Article 57 of the Egyptian Constitution issued in 1971 and repealed since 2011: Any violation of individual liberty or of the inviolability of private life of citizens or on any other rights or liberties guaranteed by the Constitution and the law shall be considered a crime, whose criminal and civil prosecution is not subject to the statute of limitations. The State shall grant a fair compensation to the victim of such violation.

3 - Law No. 175 of 2018 on Combating Information Technology Crimes.

4 - A Report issued by the Joint Committee of the Communications Committee and the Offices of Constitutional and Legislative Affairs, Defense and National Security in the Egyptian Parliament, on May 2018.

5 - Article (25) of the Anti-Cyber and Information Technology Crimes Law No. 175 for 2018, regarding Crimes on Infringement of Privacy and Unlawful Information Content: “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.”

6 - “An old trial for a new space; A reading of the judicial ruling issued in the TikTok girls case” An analytical paper issued by Masaar - Technology and Law Community

7 - During the "Tik Tok Girls" case – No. 1047 in 2020, Financial Misdemeanors of the Economic Court in Cairo, No. 246 of 2020, the Economic Appellant Misdemeanor in Cairo – the court has attempted to define the crime of violating the values of the Egyptian family, which came in the context of texts related to the protection of the privacy of individuals. The court said it was: “The use of information technology, networks, or the Internet broadcasting, sending or addressing individuals, in a manner that destroys family bonds, or underestimates productivity of the family, or entices disharmony among its members, or undermines the rules and principles that govern it.” The misinterpretation of the concept of family values as one of the provisions protecting the right to privacy,
due to the unclear wordings r who has been relied upon
While writing the texts of the Anti-IT Crimes Law No. 175 of 2018.

8 - Personal Data Protection Law No. 151 of 2020, published in the Official Gazette No. 28 bis (E) on July 15th, 2020.

9 - Article 4 of the articles of issuing Personal Data Protection Law No. 151 of 2020: “The Minister of Telecommunications and Information Technology shall issue the executive regulations of the annexed law (the “Executive Regulations”) within six (6) months from the effective date of this law.”

Articles 25 and 26 of the law have addressed, in full details, the various forms of violations on private life, and in spite of the importance of explicitly texting different forms to protect the privacy of users, that step has not been completed.

The unclear wording of the texts of the law have resulted in the protective texts such as Article 25 to become the reason and justification for the arrest and investigation of a number of users of entertainment applications, which is what has happened in the case known as " The TikTok Girls Case", where the investigation and litigation authorities have misinterpreted the text of the article, which has eventually led to the relative disruption of the texts which might have – supposedly – provided some protection for the right to privacy .

On the other hand, The Personal Data Protection Act , issued, in the middle of 2020, contained a number of rules that provide protection for partially or completely electronically processed data. Despite the importance of such law and its rules, as an important step towards protecting the privacy of the users, the law has not yet been enforced for many reasons, where the legislative structure of the Personal Data Protection Law has not been completed, as the executive regulations of the law have not been issued even though six months have passed since the law was passed . This is in addition to the fact that effective law enforcement needs to start establishing a specialized commission; The Personal Data Protection Center, to follow up the implementation of the law by the various authorities and to receive complaints related to its application, in addition to the need to address government agencies and various sectors in order to begin to adjust their situation in accordance with the obligations indicated by the Data Protection Act, all of which has not happened yet.

Existing legislative problems

One of the most significant problems facing any process related to legislative reform in Egypt, is the inability to make a precise and clear inventory of the legislations related to a specific field, as the legislative machine is constantly working to process all the details related to a particular subject according to legislative rules, to find out – by time – that there is more than one text addressing the same legal issue, and that all these rules are applicable to the same one case.

This crisis has recently developed, perhaps out of precaution and emphasizing a set of rules of which enforcement had to be ensured, regardless of which law would be applied.

It is therefore difficult to work on a legislative review that is inclusive of all legal texts, while it might be more possible to refer to the legislative features related to laws regarding the right to privacy, with examples of these features in more than one law, and explaining the importance and impact of these texts in practice together with the obstacles that these features may represent that might disable or slow down the effect of the texts that protect the right to privacy.

Unspecified technical powers for national security authorities

The laws related to communications technology, include broad extensive technical jurisdictions for the Egyptian National Security authorities , as the Egyptian Telecommunications Regulatory Law No. 10 of 2003, established the role of the Egyptian National Security authorities to obtain technical jurisdictions to carry out its tasks, especially in exceptional circumstances, such as in case of wars and pandemics.

However, the law opened the door to these authorities to operate without clear and specific rules that are not subject being monitored in terms of the extent of their legality, since the wording of the texts has given technical jurisdictions of which the limits cannot be known.

Some of these texts have an exceptional character that can be measured and determined, such as: disasters and wars. However, they also include other cases that cannot be defined, such as the use of technical capabilities for cases related to national security.

For example, Article 64 of the Egyptian Telecommunications Law , obliges service providers or operators, to provide – at their own expense, and within the authorized telecommunications network – all technical powers (equipment, systems, software and communications) that allow the armed forces and national security services to exercise their jurisdiction, within the limits of the law.

The Telecommunications Law has not specified the nature of these powers, however, the text of the article has expressly indicated that these services that service providers are obligated to provide, must take into account the sanctity of the private life of citizens, which is an indication that these powers would possibly infringe the right to privacy.

The legislative approach approved by the Telecommunications Regulatory Act has continued, in the recently passed laws, which expanded the granting of powers to national security authorities, which is evident by reading the Anti-Cyber and Information Technology Crimes Law No. 175 of 2018, where Clause 3 of Article No. 2 refers to the obligations and duties of service providers:

“Subject to the sanctity of private life guaranteed by the Constitution, service providers and their affiliates, are obligated to provide – upon the national security authorities, and as per their needs – all the technical powers that allow these bodies to exercise their competencies in accordance with the law .

It is noted that the text of Article 2 of the Anti-Cyber and Information Technology Crimes Law, has expanded the powers granted to national security agencies, since while it was talking about _unspecified_ powers that the authorities exercise within “the limits of the law”, the wording of the law came to give undefined powers as well. However, such powers were exercised only “as per the needs" of the national security services.

Such wording related to the powers of national security agencies, which have evolved over time in a direction that makes it difficult to determine the nature of such powers or the controls related to the exercise of those powers by those authorities, making it difficult to monitor the legality of the practices followed by these authorities, which constitutes a legislative restriction in order to ensure the privacy of users.

Multiple powers to monitor communications

Egyptian laws include texts that allow monitoring of communications in their traditional sense, and also allows for mass surveillance practices, or more precisely, random monitoring of social media.

There are many reasons and motives justifying these actions, including some texts of an exceptional nature, such as the powers stipulated in Clause Two of Article 3 of Emergency Law No. 162 of 1958, which gives authority to the President of the Republic whenever a state of emergency is declared , to take appropriate measures to maintain security and public order, and in particular, order to monitor messages of any kind, monitor newspapers, bulletins, publications, editorials, drawings and all means of expression, publicity and advertisement before they are published, or seize, confiscate, disable and close their places of publication.

A state of emergency has been declared in Egypt since April 2017 until now.

The state of emergency is renewed every three months, through a decision of the President of the Republic and the approval of the Parliament to the extension decision. The declaration a state of emergency has multiple effects related to violating the rights and freedoms of individuals, such as: the text related to the monitoring of communications and all means of expression, and the trial of violators before a judiciary of an exceptional nature - such as emergency state security courts – to adjudicate crimes resulting from the commission of any crimes in common law referred to it by the President of the Republic.

Although some provisions of the Emergency Law, have been ruled unconstitutional, as they violate the private lives of citizens, there are other texts that still exist and are applied until now.

An example of the ruled unconstitutional provisions is the repeal the first item of Article No. 3 which allows the President of the Republic to take appropriate measures to maintain security and public order, including: The arrest and detention of suspects or dangers to security and public order, and authorizing the search of persons and places without being bound by the provisions of the Code of Criminal Procedure.

The Constitutional Court has indicated that the text authorizing the search of persons and places without restriction or control, especially judicial authorization

represented an infringement on the rights and personal freedoms and the sanctity of private life guaranteed by successive constitutions.

An example of the still active texts is the text related to the control of means of communication and all means of expression, although it violates many rights protected under the Egyptian constitution, including texts that provide protection for private life, as well as the text that guarantees freedom of expression in all its forms and manifestations.

10 - Telecommunications Regulatory Law No. 10 of 2003 defines the concept of national security agencies, where Article No. (1) Clause 20 states: "National security agencies: include the Presidency of the Republic, the Ministry of Interior, the National Security Authority and the Administrative Control Authority."

11 - Article 64 of the Egyptian Telecommunications Regulatory Law No. 10 of 2003: "Telecommunication Services Operators, Providers, their employees and Users of such services shall not use any Telecommunication Services encryption equipment except after obtaining a written consent from each of the NTRA, the Armed Forces and National Security Entities, and this shall not apply to encryption equipment of radio and television broadcasting. With due consideration to inviolability of the private life of citizens as protected by law, each Operator and Provider shall, at his own expense, provide within the telecommunication networks licensed to him all technical potentials including equipment, systems, software and communication which enable the Armed Forces, and National Security Entities to exercise their powers within the law. The provision of the service shall synchronize in time with the availability of required technical potentials. Telecommunication Service Providers and Operators and their marketing agents shall have the right to collect accurate information and data concerning Users from individuals and various entities within the State."

12 - Article 2 of the Anti-Cyber and Information Technology Crimes No. 175 of 2018: "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 potentials 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.

13 - news published on BBC Arabic titled: "Declaration of a state of emergency in Egypt after the bombing of two churches in Tanta and Alexandria" on April 9th, 2017

The process of monitoring and recording conversations and messages received on wired and wireless means of communication have been also organized in other laws of an exceptional nature, for example: Article 46 of the Anti-Terrorism Crimes Law No. 94 of 2015: "The Public Prosecutor or the relevant investigating authority in a terrorist crime, according to the case, may authorize a reasoned warrant for a period not exceeding thirty days to monitor and record the conversations and messages received on wired, wireless, and other means of modern telecommunications, record and film what is happening and being written in private premises or across communication and information networks or websites, and seize ordinary or electronic correspondence, letters, publications, parcels, and cables of all kinds."

The provisions of the previously mentioned article are not new, where the Code of Criminal Procedure contains similar provisions, with a difference of two points;

The first is related to the controls related to the issuance of a monitoring decision, as the Code of Criminal Procedure Law requires the issuance of a monitoring decision by the investigative judge , or the Public Prosecution Office after submitting the decision to the District Judge, in addition to the Public Prosecution reviewing the seized letters, messages, papers and recordings, in the presence of the accused whenever possible.

The second is related to the nature of the offense for which the monitoring decision has been taken, where the Code of Criminal Procedure requires that the decision to monitor wired and wireless telecommunication or to make recordings of conversations that took place in a private place, should be made when this is useful in revealing the truth in a felony or misdemeanor that is punishable by imprisonment for more than three months. In addition,

the Public Prosecution may not search anyone other than the accused or a house other than his, unless it becomes clear from strong indications that he is in possession of items related to the crime .

However, the text of Article 46 of the Anti-Terrorism Law, has not included such controls, and the most difficult thing is the general context for applying these procedures as it comes in the absence of a clear definition of the nature of the terrorist crime, or the legal dimension that may give the crime a terrorist character, where this law is applicable to all crimes, and can even be applied in cases where some acts do not rise to a crime that may result in a freedom-depriving penalty.

---

14 - The court ruled "the unconstitutionality of what was included in Clause 1 of Article No. 3 of the Presidential Decree by Law No. 162 of 1958, regarding authorizing the President of the Republic to authorize the arrest, detention, and search of persons and places without being bound by the provisions of the Code of Criminal Procedure. Case No. 17 of 15 - Judicial Case - Supreme Constitutional Court - "Constitutional" the ruling was published in the Official Gazette, No. 22 bis on June 2013 ,3

15 - Article 95 of the Code of Criminal Procedure No. 150 of 1950 and amended by Law No. 189 of 2020: "The investigative judge may order the seizure of all letters, letters, newspapers, publications and packages at post offices and all telegrams at telegraph offices and order the surveillance of wired and wireless telecommunications or making recordings of conversations that took place in a special place, whenever deemed necessary in revealing the truth in a felony or misdemeanor punishable by imprisonment for a period exceeding three months. In all cases, the acts of arrest, inspection, surveillance or recording shall be on the grounds of justified warrant, and for a period not exceeding thirty days, subject to renewal for another equivalent period or periods of time

16 - Article 206 of the Code of Criminal Procedure No. 150 of 1950 and amended by Law No. 189 of 2020: "The public prosecution may not search a person other than the accused or searches the house thereof, unless compelling evidence indicate that such person possesses things related to the crime. If useful for the establishment of the truth in relation to a felony or a misdemeanor punishable with imprisonment for more than three months, the Public Prosecution may seize All letters, messages, newspapers, printed matters, and parcels at post offices, as well as all telegrams at telegraph offices; monitor telecommunication conversations; and tape conversations made in a private place. To conduct any of the previous procedures, an anticipatory reasoned warrant to that effect must be secured from a magistrate judge upon taking cognizance of the papers. In all cases a seizure, search, or monitor warrant shall be valid for a period not exceeding thirty days and the magistrate judge may renew this warrant for an equal period or periods. The Public Prosecution may examine seized letters, messages, and other papers and records, provided that such an examination will be carried out, whenever possible, in the presence of the accused and the possessor or receiver of the seized matters and any notes made by the same shall be documented. Upon the outcome of such examination, the Public Prosecution may order the inclusion of said documents in the case file, or return them to the possessor or the recipient thereof.

Inspection Procedures and Random Searches Practices

Inspection and search practices have been increasing. Those who perform such practices and procedures related to checking the content of electronic devices, from the judicial control officers (police authorities) and what they perform from checking personal accounts, e-mail and other various activities that take place through these devices.

Here we need to differentiate between the search and inspection process, carried out by law enforcement agencies (control agencies) per the orders of the investigating authorities from one side, and between inspection and search practices of devices which are done randomly from the police forces in different gathering places, streets, squares and police ambushes (security focal points).

The Code of Criminal Procedure has a dedicated chapter to regulate the procedures for entering and searching homes and searching persons, however, most of the texts are related to physical searches, which is meant to be the search for material items related to the commission of a crime, such as papers, weapons and various tools with which the crime was committed.

The Code of Procedure has established a number of controls to ensure the protection of the privacy of individuals during the inspection process, with regard to home inspections, as the law clarified that it is not permissible to search except for things related to the crime for which evidence is being collected or investigation is taking place, and that the search process takes place in the presence of the accused or his representative whenever possible. Otherwise, it must be attended by two witnesses, who shall be, as far as possible, from his adult relatives or from those who live with him in the house or from the neighbours.

If papers are found sealed or wrapped in any other way in the accused house, it is not permissible for the judicial officer to unseal or unwrap them, and it is permissible to search everything that may have been used in the commission of the crime, or resulted from its commission, or what the crime was committed against, and everything that may be useful for revealing the truth. These items are presented to the accused, and he is asked to make his comments on them.

Finally, the Anti-Cyber and Information Technology Crimes Law No. 175 of 2018 has dedicated a specific text regulating the process of inspection and access to computer programs and databases, whereas Article No. 6 of the law gives the authority to the investigation authorities to issue a substantiated order, to the competent judicial officers, for a period not exceeding thirty days, renewable once, whenever this is useful in revealing the truth about the commission of a crime punishable under the provisions of the law, to take several measures specified in Article No. 6 of the law, including:

- Seizure, withdrawal, collection or retaining data, information or information systems.
- Tracking data and information in any place, system, program, electronic support or computer in which it is located.
- Searching, inspecting, accessing and accessing computer programs, databases, and other devices and information systems, in order to achieve the purpose of control.

It appears here that the Anti-Cyber and Information Technology Crimes Law might have expanded the powers granted to the control authorities in charge of implementing the investigation authority's decision. This is evident by the absence of guarantees established by the Code of Criminal Procedure.

For example, but not limited to, the implementation of the judicial authorization under the Anti-Cyber and Information Technology Crimes Law that allows the regulators to check all the data and information stored on the computer or any information system, which may include messages, private information or data related to the profession of the person whose equipment is being scanned, regardless of the extent to which the information or data examined is related to the crime, if any, while the examination process in the Code of Criminal Procedure, an order restricted to the investigative judge only, and the law permits them, when necessary, to assign a member of the Public Prosecution office.

The role of the controlling authorities is limited to the process of controlling and seizing without examination .

As for random inspections, which have become a routine procedure related to checking the content of phones and laptops, they are related to legal justifications different from the previously mentioned procedures in regards to inspection and examination based on a judicial order.

Random search procedures can't be described as based on a clear legal justification. However, by following up on a number of investigation procedures that take place after arresting people and checking their phones, it turns out that a number of them are based on the availability of flagrante delicto, in addition to the defendant acknowledgment of the validity of the findings of the search process, which may contribute to correcting some procedures that violate the law .

17 - Article 97 of the Code of Criminal Procedure No. 150 of 1950 and amended by Law 189 of 2020 states: "The investigating judge shall have sole inspection over the letters, correspondences, documents and other seized items provided that, whenever possible, the inspection be done in the presence of the person accused and the possessor or the person to whom such were sent shall record any observations made. The investigating judge may, when necessary, delegate a member of the Public Prosecution to sort the aforementioned documents out and may, according to the results, order the inclusion of such documents to the case file or return such to the possessor or the person to whom such were sent."

Here, it must be clarified that flagrante delicto is an exceptional legal case that gives the regulators exceptional powers, such as: arresting and apprehending people and their possessions. However, there are some controls related to the validity of these procedures, because these exceptional powers may constitute a justification for the infringement of some personal rights.

Article (30) of the Code of Criminal Procedure refers that there are four forms for the fulfilment of flagrante delicto, such as: witnessing the crime when it was committed, watching the crime shortly after it was committed, tracing the perpetrator following the crime, and if the offender is found soon after the occurrence of the crime carrying objects or having traces that indicate that he is the perpetrator or accomplice in the crime .

It is also clear that there are two basic conditions associated with the fulfilment of flagrante delicto; either is that the judicial officer (the control authority) have witnessed the case of flagrante delicto himself, or the control officer himself being able to verify the occurrence of one of the cases of flagrante delicto in the crime listed in Article 30, in addition, it is necessary that witnessing the case of flagrante delicto has been done in a legitimate manner.

From reviewing the texts related to the fulfilment of flagrante delicto and the procedural controls that must be met, we conclude that the judicial officer in flagrante delicto may not search the phone/computer of the accused, but he is only entitled to seize it, for various reasons, including reasons related to the fact that most crimes committed by phones or computers are behavioral crimes, which are difficult to be perceived by any of the senses, or witnessing the accused while committing the crime in a lawful manner. The evidence that can be relied upon in the detection of crimes related to the use of the phones or computers must be based on a legitimate procedure, where most of these conditions cannot be met.

Although the aforementioned guarantees are necessary, and it is illogic to fulfil the condition of flagrante delicto, the practical reality indicates the expansion of its application. Therefore, the texts related to it to be of the rules that may contribute significantly to the violation of the privacy of individuals.

Although it is difficult to say that these practices are difficult to control, under laws or amendments to certain laws, due to the fear of demanding legislation, since demanding new legislation often ends with more restrictions, or due to the fact that the laws in many cases are not able to address the hostile practices of rights and freedoms carried out by the regulators.

However, the text expressly nullifies the procedures resulting from any procedures that include an infringement on the privacy of individuals, has become an obligatory text to be included in laws or procedural texts related to evidence-gathering or other inspection-related procedures, because the explicit text addresses important problems, most of which are related to controls for the protection of the privacy of users, have come in the form of constitutional guarantees, that are difficult to argue as an enforceable text before some courts, despite their theoretical validity.

---

18 - Judgment issued by the Criminal Chamber of the Egyptian Court of Cassation in Appeal No. 15854 of 84 issued on the 2015/02/23 session.

19 - Article 30 and beyond of the Criminal Procedure Law No. 150 of 1950 and amended by Law 189 of 2020: "The crime shall be deemed a crime in flagrante delicto in the event caught during the commission or shortly after the commissioner. A crime shall also be deemed a crime in flagrante delicto if the perpetrator is chased by the victim or the public while crying out after the commission thereof, or if the perpetrator is found shortly after the commission of the crime carrying arms, weapons, luggage, documents or other items proving that said is the perpetrator of or accomplice in the crime, or if there are signs or indications that indicate such guilt."

20 - Article 58 of the Egyptian Telecommunications Regulation Law No. 10 of 2003: "NTRA shall prepare, manage and update a database containing the Frequency Spectrum Users Database, and such database shall be classified in order to protect the privacy of the Users."

Absence of controls on the collection and storage of user data

The Egyptian legislative environment is filled with vast contradictions, as there are many laws that represent a direct threat to user data. Despite the passage of the Personal Data Protection Act, it has not yet been enforced, as we previously explained.

Explicitly discussion of the protection of user data began in the Telecommunications Law No. 10 of 2003 which included an explicit provision that obligates the National Telecommunications Regulatory Authority (NTRA) to the confidentiality and protection of user data , the law also obligates providers and operators of telecommunications services and their authorized agents to market these services by obtaining accurate information and data about their users, from citizens and from various authorities in the country.

The law also established a penalty in the event of disclosing any information relating to users of communication networks, or what they conduct or receive from communications .

During the past three years, there has been an increasing discussion regarding a law to protect user data; The first attempt came through the Anti-Cyber and Information Technology Crimes Law, which has obliged the service provider to take some measures related to data protection. However, the law was unable to balance the considerations related to the preservation and storage of data for specific purposes and the protection of this data.

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.

Article (2) of the Anti-Cyber and Information Technology Crimes Law

The Anti-Cyber and Information Technology Crimes Law No. 175 of 2018 has initially expanded the amount of data that can be stored, by service providers, but has rather, opened the door to saving and storing non-limitable types of data according to binding decisions of NTRA, in addition to the length of the data storage period, which can be up to 180 days, which constitutes a conflict with the legal rules recently established by the Personal Data Protection Act.

---

21 - Article 73 of the Egyptian Telecommunications Regulatory Law No. 10 of 2003: "Whoever perpetrates any of the following deeds during the performance of his job in the field of Telecommunications or because of it shall be liable to a penalty of confinement to prison for a period of not less 3 months and a fine of not less than L.E. 5,000 and not exceeding L.E. 50,000, or either penalty:

1. Annunciation, publishing or recording the content of any Telecommunication message or part of it without any legal basis.
2. Hiding, changing, obstructing or altering any or part of Telecommunication message that he might have received.
3. Refraining from sending any Telecommunication message after being assigned to dispatch it.
4. Divulging without due right any information concerning Telecommunication Networks Users or their incoming or outgoing communication"

Weak procedural controls related to the protection of the right to privacy

With the increasing pace of legislation related to communication technology, there are problems related to the drafting of these legislations.

Of course, most of these problems are not new, however, it is difficult to find a reason for them due to several factors related to the timing during which these legislations have been issued. Most of such legislations have been issued in one parliamentary season, and a legislative agenda that has been issued by a specialized committee; the Communications and Information Technology Committee in the Egyptian Parliament, therefore, it is difficult to understand the lack of complementarity between these legislations.

These problems have directly impacted the rules related to the right to privacy, where they are mainly summarized in the absence of a link between legislation that may provide some aspects of protection and other legislation, as if these laws were written separately.

For example, the Personal Data Protection Law, which includes a large part of the procedural controls related to data protection, does not have a clear and coherent backer in the Anti-Cyber and Information Technology Crimes Law, as the data Protection Act adopts the rule that the process of collecting and analyzing data must be for specific purposes, already known to the user, however, the Anti-Cyber and Information Technology Crimes Law allows service providers to collect data that is not specified or limited by the law, but rather leaves such task of specification to be determined by decisions issued by NTRA, which in turn leads to the possibility of increasing or changing the type of data that is collected on an ongoing basis.

There is also a complete absence of procedural controls regarding the increasing powers enjoyed by government agencies and business institutions, that enables the understanding and analysis of user behavior. This feature has been always evident in the form of a procedural control regarding the protection of the right to privacy, and it has become clearer by examining the wordings of the rules of protection.

Most of the texts related to criminalization controls and the imposition of fines, are clearer and more detailed compared to the protective texts, of which the wordings have always been unclear or specific together with complete absence of means of compensation and redress in the event of damage, which leads the victims of violations of the right to privacy to the traditional litigation methods, which require long periods, in addition to the need for technical reports and attempting to prove the element of damage that occurred as a result of the violation, plus standing before non-specialized litigation bodies, which entails continuing for many years to obtain compensation, leading many to be reluctant to take this route.

The most important legislative determinants related to privacy-related texts

The general situation previously discussed can be summarized that it is difficult to mention all the legislative problems related to the right to privacy, while it is possible to mention the common features that can be distinguished.

22 - The report was issued at the 39th session of the Human Rights Council – Annual Report of UNHCR. Clauses 2 3 &. August 3rd, 2018. A/HRC/29/39 .

Also, proposing alternatives to deal with these problems, can be represented in legislative controls and limitations, that must be included in the legislation that will be issued in the future, or when amendments are made to existing and enforced texts.

These determinants depend in many of their angles on the conclusions of the annual report of the United Nations High Commissioner for Human Rights (UNHCR) with the title; “The Right to Privacy in the Digital Age” , which addressed the challenges related to the rules and practices that imposed themselves,

and how to deal with them. The report also monitored a number of legislative and other practical practices that pose a threat to the privacy of users in the digital age.

Therefore, the general frame of this report, which is very similar to the Egyptian situation, will be included.

Such determinants must be viewed as interrelated and complementary elements, where they must be fully taken into account, and the most important of which can be summarized as follows:

A. Clarity of legislative texts that may affect the right to privacy:

The controls on the clarity of the texts related to the right to privacy is on top of the determinants necessary to protect the right to privacy, due to the lack of clarity and contradiction of the texts, leading to wasting legislative guarantees, especially since the continuation of the legislative process in this way will be useless, and rather, possible that the text be applied incorrectly and out of place, which eventually turns the controls into a new limitation on users, like what happened in the “TikTok girls” case, where the vague unclear wording of the crime of infringing the Egyptian family values – in the Anti-Cyber and Information Technology Crimes Law,

and as one of the texts that was mainly dedicated to protecting the privacy of users – has led it to become a restriction on freedom of expression and turning it into an accusation, that constitutes entails financial penalties and freedom-depriving penalties.

B. Subjecting powers of an exceptional nature to judicial oversight:

Powers of exceptional nature are related to the first determinant, as all regulating texts – for the exceptional powers – should be included in clear and specific legal rules. Therefore, these powers and the authorities they enjoy are subject to judicial monitoring as a mandatory and basic condition for the commencement of their exercise, as well as the ability of the judiciary to exercise subsequent control over the legality of these decisions, and the limits of their exercise to the extent necessary to perform the required tasks, and the extent of harm to the persons against whom these powers were exercised.

C. Legal practices affecting the right to privacy are linked to the principles of necessity and proportionality

The principle of necessity and proportionality is correlated to many legal rules that give exceptional powers – surveillance, inspection and examination – conducted by the control authorities based on a judicial order or as an act of inference.

Such actions should be subject to controls that limit exceptional deviance – of the laws protecting the privacy of individuals – to a specific intervention that is within the limits of the judicial order and clearly justified. Moreover, no pursuits or judicial prosecutions could be based on the previously mentioned deviance. Such controls should be expressly stated, and procedures exceeding these limits should be invalid.

D. The right to an after-action notice of being monitored:

Most laws include powers that may permit surveillance for periods of time under court orders. In this case, legal protection of the private life of the person is void, without necessarily being notified. This is supposed to happen for legitimate purposes; of which the most important is revealing the truth about the commission of a crime.

As previously mentioned, these exceptional measures must be subject to the principles of necessity and proportionality, and judicial monitoring for their legality. However, the enforcement of these principles is linked to an important rule, which is the right of a person against whom no crimes have been committed and whose privacy has been violated, to be at least aware that he is being monitored.

E. Providing simple legal means of compensation for damages:

Generally, there are many procedural complications related to redress after harmful practices, of which the most important is compensation for violating the privacy of users, where this requires procedures related to establishing the act that constitutes an infringement of privacy, to establish the damage caused by this infringement, in addition to the necessity of providing technical evidence and expert opinions, and the need for a court specialized in these disputes.

Hence, the existence of independent bodies – through which the act of infringement can be established, as well as providing technical evidence and the necessary legal assistance as a first step for litigation, plus the specialized courts for such disputes – may contribute to simplifying the legal procedures and shortening the litigation period which may last for many years.

F. Moving forward with completing legislative rules and establishing independent monitoring bodies

Continuing the process of legislative construction of laws and regulations that provide protection for the privacy of users is very crucial as a primary step to move from the state of complete absence of rules, and in turn the possibility of conducting an integrated critical evaluation of these rules as a whole, and eventually the possibility of offering alternatives to these rules.

However, there is always a great deal of fear in terms of demanding legislations or amendments.

Therefore, the construction process must be completed with the participation of the various concerned parties and representatives of relevant civil society entities. Moreover, the aforementioned legislative determinants should be taken into account, and the legislative errors that have occurred should be addressed, as much as possible.

The steps that need to be taken in future are:

Completion of the proposal related to the executive regulations of the Personal Data Protection Law, provided that the criticism of the law is addressed and the legislative construction is accomplished and completed by establishing the relevant independent bodies, such as: The Data Protection Center.

---

23 - A legal paper entitled: "Personal Data Protection Law. Enhancing the right to privacy or delusion of improving the legislative environment" issued by Masaar - Technology and Law Community, on December 5th, 2020 .

Conclusion

The Egyptian legislative system suffers from contradictions that restrict the individual right to privacy. This system also works in an incomplete manner that squanders any positive efforts to protect the data and private lives of individuals. Such legislative contradictions indeed result in the transformation of some guarantees of protection of the privacy of individuals into restrictions on this right.

Moreover, many security and administrative authorities have many powers that authorize the overriding of the constitutional protection for privacy. Such powers need serious legislative review, so that the exceptional powers – which are necessary to be maintained – should be subject to the judiciary monitoring, to ensure that the authority is not abused by the authorities that have these powers.

The authorities should also establish clear limitations regarding the control authorities in regards to arrests, searches and surveillance of communication devices of individuals, to ensure that the law enforcement operations do not turn to be an opportunity to violate the privacy of individuals and that the procedures affecting the privacy of individuals are within the limits of the judicial permissions it authorizes.

The legislator should as well obligate the authorities – allowed to interfere in the privacy and private lives of individuals in specific circumstances – to notify the target people that they are being monitored, as to enable them to claim compensation in case such monitoring exceeds the limits set by the Constitution and the law.

Also, the authorities should provide simplified means to compensation for violations of the right to privacy carried out by the government or companies, and remove all obstacles that hinder the proof of such violations or prolong the redress for the victims of these violations.

https://masaar.net