TECHNOLOGY & LAW COMMUNITY

PERSONAL DATA PROTECTION LAW

Does it Really Aim at Bolstering the Right to Privacy?

OR

Is it an Attempt to Give the Illusion of an Improvement in the Legislative Environment?

https://masaar.net

PERSONAL DATA PROTECTION LAW

Does it Really Aim at Bolstering the Right to Privacy?

Or

Is it an Attempt to Give the Illusion of an Improvement in the Legislative Environment?

Contents

Introduction

Egyptians generally suffer from weak legal protection to their 'right to privacy'. In connection to this, and as regards the data collected by the government during daily administrative dealings, and the data collected by private companies from their clients, there exist several legislative loopholes that allow for personal data disclosure without consent of the data subject.

Considering this situation -the lack of a legislation that protects the privacy of personal data- the Egyptian civil society has called all through the past two decades for a legislative intervention to fill the gap.

Lately, the Egyptian authorities adopted a bundle of legislations related to the organization of the use of information technology. However, this legislative intervention was not for the sake of protecting individuals' right to privacy, as much as it was for the sake of controlling digital space: after two and a half years spent by the communications committee in the Egyptian house of representatives to discuss the personal data protection draft law, the house finally approved it, then the president ratified it last June.

Private companies working in the communications sector were widely involved in the draft law's discussion process, unlike civil society organizations whose participation was marginal.

On the other hand, it is interesting that the personal data protection law's jurisdiction is limited to organizing electronic data only, even though most daily dealings, either with the government or the private sector, are based on the disclosure of personal information that is not digitally processed. There are no other legislations that handle the protection and sharing of non-digital information. This testifies to the fact that the personal data protection law endorsement was not really meant to protect individual privacy, but that it is a tool to address the international community with the claim that Egypt has a legal environment prepared to make global investment partnerships in the information technology sector.

The Egyptian legislator modelled the personal data protection law on the European General Data Protection Regulation (GDPR). However, he amended the GDPR regulation in a way that 'compressed' some of the law's articles, especially as regards the individuals whose personal data is shared with different parties. The law also referred the final say as regards a wide range of data protection activation procedures to its 'executive regulations' which is not issued until now.

Despite all this, the law should be considered an important legislative step forward that needs intensive efforts for it to be implemented.

Massar thinks that the basic thing that matters when it comes to making the personal data protection law an effective tool for protecting individual privacy, is the philosophy of the legislation itself. The Egyptian authorities venture to organize the process of information sharing must start from a genuine belief in the right of individuals to privacy, not only from an ambition to ameliorate the investment environment. However, an attentive reading of the law's articles shows that the right to privacy was not the prime motive behind its adoption; rather the prime motive was creating a legislative environment that is attractive to financial aid packages in their different forms. This is a legitimate goal, but it must not come at the expense of the right of individuals to privacy which is protected by both the Egyptian constitution and the international law.

The personal data protection law (no. 151 for the year 2020) defined 'personal data' as follows: "Any information relating to a natural person who can be identified, or is identifiable, directly or indirectly, by reference to an identifier such as a name, a picture, a voice, an identification number, an online identifier, or any information that defines the psychological, health, economic, cultural or social factors specific to the identity of that natural person".

However, the data protection law exempted some agencies and institutions from submission to its jurisdiction, for example the central bank and the national security bodies. The legislator should have exempted some but not all types of information held by these agencies and institutions. This wholesale exemption is a violation of the principle of the rule of law, as all natural and legal persons should submit to the legal commitment of protecting individual privacy.

This Massar commentary is written amidst an incomplete legislative context since the Egyptian government is still to issue the executive regulations of the law. The coming period might also witness the formation of the Personal Data Protection Center (PDPC) and its different committees. Hence, this commentary focuses on analyzing the most important articles of the law, noting on some of their legal formulations. It will also review the legislative context in which the law was endorsed, and the aims pursued by the legislator in issuing it.

It should be noted here that the review carried out by this commentary bases itself on three sources and manuals: the parliamentary reports issued by the communications committee during the discussions of the draft law, the explanatory memorandum accompanying the government-proposed draft law, and the standards pertaining to the formulation of data protection laws stated in "The Legislator's Manual to the Personal Data Protection Law" issued by Access Now organization.

The Addressees of the law

The personal data protection law commits the individuals and agencies that might retain users' personal data -either this was due to the nature of their job or due to any other reason- to certain basic commitments. In this regard, the law differentiates between the disparate commitments according to the nature of the entities that deal with personal data. And despite that the law gives a lot of attention to clarifying the various forms of dealing with data -holding, controlling and the different ways of processing- and to the legal responsibilities of the holder, controller, and processor, yet it did not give enough or detailed attention to delineating the rights being protected, and the measures that can be taken by citizens if their rights were breached. In short, the law focused basically on those who uphold the data, not on the individual citizens giving away their personal data.

The law defines the data holder as follows: "any natural or legal person who legally or factually holds and retains personal data in any manner, regardless of whether that person collected that data initially or received it by way of a transfer". It then differentiates between the various agencies that hold data.

The law on the other hand defines the controller as follows: "a natural or legal person who has the right, due to the nature of his work, to obtain personal data and to determine and control the process and criteria of holding, processing, or controlling data".

Lastly it defines the processor as follows: "any natural or legal person mandated by his job to process personal data for his own benefit or for the benefit of the controller (in agreement with the latter and according to his instructions).

The aim behind endorsing the personal data protection law

There is no clear legislative policy pertaining to the communications and information technology sector to help us understand the needs and priorities according to which information technology laws are issued. Hence, this commentary depends on the press statements of the members of the parliament's communications committee, in addition to the law's explanatory memorandum and the relevant parliamentary reports, to try to delineate the aim behind endorsing the personal data protection law.

Members of the Egyptian 2020-2015 parliament's communications committee gave several press statements that say the committee would focus on endorsing three basic laws: the electronic crimes law (issued in the third quarter of 2018), the personal data protection law (issued at mid2020-), and the free circulation of information law (its draft was sent to parliament at mid2018-, but it is not issued until now).

Parliamentary discussions and statements stressed that these three laws, which are closely interconnected, should be endorsed urgently. No obstacles stood in the face of endorsing the electronic crimes law; it was formulated to give the law enforcement entities a free hand in the cyberspace, by way of legalizing anti-human rights and anti-basic freedoms practices, and by way of criminalizing the free expression of thought on the internet (this law's articles were later frequently used to direct criminal charges against citizens whose only crime was to practice freedom of expression on the internet). On the other hand, the personal data protection law, which puts restrictions on the governmental bodies' use of personal data, was delayed until late in 2020, while the third and last law, the free circulation of information, was indefinitely postponed for unknown reason.

A social need to endorse a law that provides protection for citizens' personal data was not the basic aim behind ratifying the personal data protection law. The parliamentary and governmental discussions prior to its endorsement mentioned different goals, including that its ratification would upgrade Egypt's position in the international human rights scale. The law's explanatory memorandum also adds goals related to the economic revenue expected in case of its ratification. It says that knowing the economic value of personal data comes from the huge data analysis processes, and hence protecting data enhances the outsourcing business and the data centers industry, both considered high-surplus-yielding activities (this in its turn creates and attracts more jobs and investments).

The same argument was reiterated in the parliament's communications and national security committees joint report. It said that the state's encouragement of investments in the huge data centers industry will help Egypt to become "a global dataway": "and since fulfilling this aim necessitates the presence of a proper legislation, this law intends to enhance the business environment in Egypt and improve the international reputation of the government's administrative performance".

Widescale exceptions to the law

The personal data protection law was endorsed late in time: at the end of the last round/year of the 2020-2015 parliament. Discussions on its draft started at the end of 2017 and ended at the beginning of 2020, and then, after this legislative marathon, the president of the republic ratified it in June 2020.

This delay is due to objections raised by several of the state's administrative/security bodies, among them the Egyptian Ministry of Interior. The parliament's communications and information technology committee held a meeting at the beginning of 2018 with the representatives of the ministries of 'interior', 'defense', and 'foreign affairs' to decide on the articles of the law related to national security. The committee ended its deliberations by stating that the law would not be applied to the ministries of interior and defense, as it was feared that the law's regulations would be applied to information gathered by the ministry of interior, especially data pertaining to cases of drug dealing and terrorism, and information on prisoners, various religious sects, and the demographic composition of the population.

Despite the communications committee's decision to exclude national security agencies from the law's jurisdiction, yet it was the case that the first draft (proposed by 60 MPs) was abandoned and replaced by another, government -worded, draft. This government's proposition respected the national security red lines, but this did not prevent other governmental agencies from objecting. In June 2019, the Central Bank of Egypt (CBE) sent a letter to the parliament's speaker demanding that the personal data of the bodies that are audited by the CBE (the banks) should be exempted from the law's jurisdiction to evade any conflict in jurisdiction between the CBE and the PDPC.

The parliament concluded by approving a number of exemptions to certain kinds of data and certain kinds of entities from the jurisdiction of the law. The third article of the law specifies the exemptions as follows:

Personal data held by natural persons for others and is processed for personal use.

- Personal data processed for official statistics or to apply a legal text.
- Personal data processed solely for media purposes -on the condition that it is true and exact- subject to media laws and regulations.
- Personal data related to judicial reports, investigations, and claims.
- Personal data in possession of the national security agencies. PDPC is obliged -if requested by a national security agency- to notify the controller (or the processor) to modify, delete or hide certain personal data for a certain period. The controller and the processor have to carry out what they are ordered to do.
- Personal data in possession of the CBE and the entities audited by it, except for the money transfer and money exchange companies, subject to data protection rules under the banking laws and regulations.

The exceptions stated in the data protection law were based on two criteria: the first is the nature of the data (for example the statistics gathered by the Central Agency for Public mobilization and Statistics and the data processed for personal use is exempted). The second criterion is the nature of the state administrative body at hand (certain bodies are exempted completely from submission to the law).

Regarding the second criterion, the law gives undefined powers to certain state bodies to hold data and process it with no judicial supervision. These absolute powers are unimaginable, especially that there are no legislative criteria that sort the data collected by the national security bodies according to their nature. It is understandable of course that some of the data processed by these bodies cannot submit to the law because of their nature. But this should not mean that all data acquired by national security bodies is sensitive and cannot be under the rule of the personal data protection law. Exceptions should be stated, restricted, and explained.

In addition to this, the law exemptions' umbrella goes beyond national security to cover other state bodies like the CBE and the entities it audits. This is not understandable, and it weakens the law to a great extent. Excluding the whole of the banking sector from submitting to the data protection law does not only contradict the basic rights stated in article 57 of the Egyptian constitution (protecting the right of people to privacy), but it also runs counter to the goals stated by the legislator to explain the necessity of the law: to attract international investments.

Users guarantees and rights during collection and processing of data

The personal data protection law gave certain guarantees as regards the rights of the users.

(The 'user' is called by the law the 'data subject'). These guarantees are the basic rules to be followed during the process of collection and processing of personal data. And despite the clear importance of these 'guarantees' -they should be considered the main aim behind issuing the law- yet they were very briefly worded. The law stated the basic guarantees/rights without detailing the connected concepts or the specific regulations. Also, the articles dealing with these rights were spread through the text of the law in different forms. They were unclearly mentioned in the article pertaining to "the rights of the data subject and the rules of collecting and processing of data". Then they were partly mentioned in the article pertaining to the responsibilities of the controller and processor. And finally, they were mentioned in the form of conditions and regulations related to the process of data collection. This leads to confusion and makes it difficult for the law addressees to understand their rights.

Article 2 of the law is the main article in which users' guarantees are delineated. It runs as follows:

"It is inadmissible to collect, process, reveal, or disclose personal data in any way without the clear consent of the data subject, or in legally approved instances. The data subject has the following rights:

1. The right to know what personal data is acquired by any holder, controller, or processor, and the right to request access or a copy of the personal data being processed.
2. The right to give and withdraw consent to the collection and processing of personal data.
3. The right to correct, delete, change, update, or add to personal data.
4. The right to request the restriction of processing of personal data to a certain range.
5. The right to know when personal data is illegally accessed or breached.
6. The right to protest the processing of personal data and any results of such processing if it contradicts or violates users' fundamental rights and freedoms.

Except for item 5 above, the data subject should in all cases pay the cost of the service provided to him by the controller or the processor in relation to the exercise of his rights. CPDP is to decide the price of the service on the condition that it does not exceed EGP 20,000.

The text of the above-mentioned article 2 (the main article where the rights of the data subject is stated) shows that there are some guarantees that are neglected by the law:

The right to know if personal data was illegally accessed or breached:

Article 2 of the personal data protection law guarantees the right of the data subject to know if his personal data was breached. However, it does not specify the exact way in which the data subject would be notified of the breach, or the time limit during which he should be notified. Also, despite that the text of article 7 -pertaining to the responsibilities of the controller and the processor- organized the way in which those whose rights were violated would be notified of the violation, yet it stated that only the PDPC, and not the data subject, should be notified within a range of 72 hours. And if the violation is related to a national security issue, notification to the PDPC should be immediate, and the PDPC, in its turn, should notify the national security bodies immediately; all this without mentioning a time frame in which the data subject should be notified.

The right to know the aim behind collecting and processing data:

Article 2 of the law gave the data subject the right to know what data is acquired by any holder, controller, or processor, and the right to request access or a copy of the data being processed. However, it dropped out the users' right to know the aim behind collecting data, making this 'right' just one 'condition' among others that should be fulfilled during the first time data is collected. In connection to this, article 3 of the law stated that data should be collected for specified legitimate reasons "that are disclosed to the data subject". This formulation has its important consequences, which are that the requirements for data collection came in a vague text that allows only for one notification to the user. This shows the difference between the formulation of the aim behind data collection as a responsibility on the controller and its formulation as a right to the user. Organizing the aim behind collecting data as a right to the user means guaranteeing his right to continuously exclaim about his collected/processed data, whatever the phase of data handling is. The initial acceptance is not enough, and it should not be considered an approval to collect additional data afterwards. Continuous and complete knowledge on the side of the user is a basic guarantee for the data subject who has the right to object or withdraw his initial acceptance.

High fees

The law puts an upper ceiling to the price to be paid by the data subject in exchange for any service provided to him by the controller or the processor as regards practicing his rights. This ceiling is EGP 20,000. This high fee raises fears as regards the inaccessibility of the cost of a service provided to the end user. This means that the data subject might find it difficult to exercise his rights.

But this problem can be overcome by pricing the different services of the PDPC, as the law did not give a lower ceiling for the cost of services. Hence, the PDPC should price its services in a way that balances between the effort exerted in their provision and the economic abilities of the users.

Data access procedures

One of the prime aims behind the data protection law is to give the user accessibility to the data upheld by the controller, processor, or holder. This is a cornerstone that allows for the activation of all the other rights of the data subject, mainly the rights to delete, correct, or amend the data. Hence, the rules pertaining to the accessibility of data should be noticeably clear and outspoken.

Article 10 of the law organizes this matter. It says:

"The controller, the processor, and the holder are committed to the following procedures when and if the user requests access to his personal data:

1. The request should come in the form of a written application, handed out by the user himself or somebody who has the right to do so.
2. The needed documents should be presented by the user.
3. The request should be processed within 6 working days, and if it is denied, the reason should be specified (if the PDPC did not respond in 6 days, this should be considered a rejection)."

Convenience of accessibility

As we can see, article 10 did not specify the way in which a users' request to access data would be fulfilled. It only stated the time limit within which the response to the request should be delivered. This needs to be rectified and the article's text needs to be clearer as regards the way in which the data access request would be fulfilled. For example: the data should be accessible in clear and understandable language and should be delivered in the format determined by the user (either in paper or electronic form), and if electronic it should be available in a simple and widespread digital format.

Rules pertaining to the disclosed data

Article 10 of the law also did not specify the rules pertaining to the response to the data access request. The controller or the processor should clarify in the response the state of the data that is requested: if it was processed, or shared with other parties, and for how long it was stored, and the ways in which it was used.

Lack of data correction, amendment, or deletion procedures

Furthermore, article 10 organized the procedures related to giving access to data, but it did not mention any procedures to be followed in case there is a request to correct, amend, or delete personal data. It is true that article 12 commits the controller/processor to correct any mistake in personal data "as soon as he is informed of it". However, it did not organize the procedures and mechanisms pertaining to filing requests for correction, amendment, or deletion of data.

Responsibilities of the controller, processor, and holder

The data protection law grants the user a number of guarantees as regards the protection of his personal data. These guarantees are drafted in the form of responsibilities to be fulfilled by all processors, controllers, or holders of data. The law differentiates between the responsibilities of the controller and those of the processor, but it drops out the responsibilities of the holder.

Article 4 of the law organizes the commitments of the controller.

They vary between commitments pertaining to users' rights (consent of the user, ensuring the accuracy and suitability of data to the intended purpose, deletion of data after end of purpose, correcting any mistakes in data), and other general commitments (acquiring a license from PDPC, Devising the suitable criteria and methods of data processing, ensuring the consistency between the aim behind data collection and the way of its processing, taking all needed technical and organizational measures to protect and secure data from any breach or sabotage, keeping a register of data that includes description of its categories with a clear statement of the ways and the time ranges of their use and of the mechanism of deletion or amendment, in addition to any information as regards data transfer across borders, etc.). And finally, and as regards a controller residing outside Egypt, the law obligates him to appoint a representative in the country. (All details of the policies, measures, regulations, and technical standards to be followed by the controller are referred to the law's executive regulations which is not issued until now).

No mention of the responsibilities of the data holder

The personal data protection law did not clearly define the data holder. It also was unable to differentiate between the holder, and both the controller and processor. So it defined the holder as any natural or legal person who holds legally or actually personal data in any form. The law also stated how the process of data access from the holder would be carried out (article 10). However, chapter three of the law organized the responsibilities of the controller and the processor only, without any mention of the holder's responsibilities.

Basic commitments during the process of data collection

The data protection law did not allocate an independent section to delineating the regulations pertaining to the basic information the user should be informed of while collecting his data.
It found it enough to state only the basic measures by which the controller and processor should abide.

These measures are: keeping a register of the data on the condition that this register includes a description of the data at hold, who would access it, for what long, in what range, and the methods of data deletion or amendment. This means that the responsibilities of the controller and the processor are considered internal administrative responsibilities (for the purposes of follow up and auditing by PDPC). The law did not commit the controller/processor to any procedural measures pertaining to the rights of the data subject. In fact, the commitments on the controller and the processor as regards data collection should have included providing the user in writing with the following information:

Contact information of the data protection officer representing the controller and processor.

- The aims behind the kind of processing that would be carried out.
- The time interval during which the data would be stored.
- The measures needed to retrieve a copy of the data.
- The measures pertaining to the correction, amendment or deletion of personal data, and the measures pertaining to the restriction of data processing range, or to the wholesale objection to processing it.
- The measures needed to withdraw consent on data collection.
- The measures needed to contest any of the decisions to amend, delete, correct, or transfer data.
- Possibility that the processing of data might be carried out by parties not subject to Egyptian laws.

Data sharing across borders

Data transfer and sharing is not only a national matter that occurs between governmental agencies/companies within the borders of one country. Transactions across borders and the signing of inter-state agreements that allow for data sharing are becoming a daily routine. This means there is a possibility that violations might occur, especially that the Egyptian data protection law did not devise clear standards that represent the minimum that should be met during data transfer across borders.

The data protection law stated two conditions in case of data sharing across borders: the first is that there should be a level of protection of data in the host country that is no less than the protection guaranteed by the Egyptian law, and the second that there should be a permit given by the PDPC to allow for data transfer across borders.

Articles 14 and 15 of the law organize data transfer across borders:

Article 14: "It is forbidden to transfer collected or ready for processing data to a foreign country unless this country has a level protection not less than the level guaranteed by this law, and after being granted a permission from PDPC. The policies, standards, criteria and regulations needed to transfer, store, share, process or access personal data across borders are to be decided by the executive regulations of this law".

Article 15: "As an exception form the rulings of article 14 of this law, it is admissible in case of a clear consent from the data subject (or whoever acts on his behalf) to transfer, share, circulate or process data in another country that has a lower level of protection than that delineated in the previous article, in the following cases:

1. Safeguarding the life of the data subject and providing him with the needed medical care or health services.
2. Carrying out commitments that prove or defend a right in front of the justice system.
3. Concluding a contract, or executing an already concluded contract, between the processor and others, in the benefit of the data subject.
4. Executing a measure pertaining to international judicial cooperation.
5. Carrying out a legal commitment to protect public interest.
6. Transferring money to another country according to its legislations.
7. If the transfer or circulation of money comes to execute a bilateral or multilateral agreement that Egypt is part of.

The rules stated in the Egyptian law to protect data sharing across borders are not enough

The data protection law dealt with rules of data sharing across borders in a brief manner. It did not mention the regulations related to assigning the range of responsibility of the different parties. Also, the law limits its requirements for data transfer to the existence of a legislation that provides no less protection than the Egyptian law. However, there are other conditions that should be met like: respect of the host country to the rules of human rights and basic freedoms, presence of an independent agency working on executing the data protection law, and other conditions pertaining to the daily practices and not only to the legislative codes.

Exemptions to the rules of data transfer

As we mentioned earlier, article 15 of the law deals with the exceptional cases that are exempted from following the rules pertaining to data sharing across borders. Exceptions are allowed in cases where the users give consent and express need to share their data with parties that do not necessarily abide by the data protection rules. However, the law did not commit the CDPC to inform the users of the possible hazards to be expected in case of sharing data with parties that do not fulfill the rules stated in the Egyptian data protection law.

Lack of the needed policies and regulations for data transfer/sharing/access/storing across borders

The data protection law referred the rules pertaining to the criteria of data sharing and access across borders to its executive regulations. This is a legislative error that should be rectified. The protection of data is supposed to be the main aim behind endorsing the law. Hence, it is not proper to refer some of the data protection rules -in this case: data shared across borders- to the executive authority, or to allow for their continuous change without informing the user.

The role of the CPPC in case of complaints

Sharing and accessing data across borders can involve violations and unacceptable disclosures. This might entail taking legal measures like filing complaints, and maybe even resorting to courts. Hence, there is a need for clarity as regards the jurisdiction of the Egyptian vs. the host country judicial systems in case a dispute erupts. This also raises the question of executing Egyptian court rulings outside the borders, another issue the law did not deal with. And finally, the law did not clarify the role of PDPC in following up on the execution of relevant court rulings.

Investigation

The law did not mention the role of the PDPC in investigating complaints filed against parties residing outside Egypt. It also did not show how the PDPC would assist or inform users of lists of the countries, corporates, and organizations that respect the data protection rules (a thing that necessitates that the PDPC periodically surveys the developments in different countries and organizations).

Composition and jurisdiction of the PDPC

The personal data protection law organized the rules pertaining to the composition and role of the agency entitled with protecting personal data. This agency is called Personal Data Protection Center (PDPC), and it is assigned the role of fulfilling all the tasks related to the execution of the personal data law. Article 19 of the law deals with the PDPC's formation and functions: "the PDPC aims at protecting personal data while being collected, processed and accessed".

The PDPC's jurisdiction includes unifying data protection policies in Egypt, issuing licenses, permits, and approvals pertaining to the application of the law, approving consultants who are entitled to provide advice on data protection procedures, coordinating with governmental and non-governmental entities to guarantee protection of data, contacting the relevant data protection initiatives, working on improving human resources in and out of the government as regards data protection skills.

Moreover, the PDPC has the jurisdiction to receive complaints related to data protection breaches, inspect and supervise the various addressees of the law and take the needed legal measures, make sure of the fulfillment of the conditions of data transfer across borders, give the needed expertise and consultancies as regards data protection (especially to the judicial authorities), make deals and agreements for cooperation and coordination with international parties, and prepare an annual report on the state of data protection in Egypt.

The special nature of the PDPC

The data protection law states that the PDPC is "a public economic agency". However, the jurisdiction and functions of the Center say it is a 'services' not an 'economic' agency. This formulation reflects the legislative philosophy behind the law. The legislator's eye is on the economic revenue that can be reaped from data protection, while it should have been on guaranteeing the interests of the data subjects.

Composition and independence of the PDPC

Article 20 delineates the formation of the PDPC. It runs as follows:

"The PDPC should have a board headed by the designated minister and its members are:

1. A representative of the Ministry of Defense to be chosen by the minister of defense.
2. A representative of the Ministry of Interior to be chosen by the minister of interior.
3. A representative of the general intelligence to be chosen by the head of the agency.
4. A representative of the Administrative Control Authority to be chosen by the chairman of the authority.
5. A representative of the Information Technology Industry Development Agency to be chosen by the head of the agency's board.
6. A representative of The National Telecommunications Regulatory Authority to be chosen by the head of the authority.
7. The executive director of the PDPC.
8. Three experts to be chosen by the designated minister.

The board membership term is 3 years subject to renewal.

The prime minister is to issue a decree stating the composition and financial compensations to the PDPC members.

The PDPC board has the right to form one or more committee and temporarily assign to it/them some tasks. The board also has the right to delegate some of its powers to the chairman of the board or to the executive director".

As we can see, the law adopted a certain method to choose the board members of the PDPC: direct nomination by the relevant administrative bodies. There is no mention of the criteria (for example: certain level of expertise) of choice.

Most of the board members on the other hand represent administrative bodies, no representation to the interest groups or the civil society organizations. The security bodies for example fill nearly half of the seats of the board (4 out of 9), which is unfathomable considering that national security agencies are exempted from submission to the law.

Moreover, the law did not state explicitly that there must be no conflict of interest between the administrative posts held by board members and their role in administering the PDPC.

All this leads to the conclusion that the PDPC is not an independent entity, and it will be difficult to ensure there would be no interference in its affairs.

Conclusion and recommendations

Endorsement of the personal data protection law is an important step on the way to safeguard users' privacy. This becomes all the more important when we remind ourselves of the poor legislative environment prevailing in Egypt; an environment lacking any guarantees as regards the privacy of individuals. All this in addition to the lack of regulatory rules as regards the measures needed to protect personal data, and to the vagueness of justice seeking rules in case any breach occurs.

On basis of the observations mentioned in the current commentary, Massar recommends the following:

- In order to make the personal data protection law effective, the Egyptian authorities should carry out a thorough legislative revision of all the other laws that organize daily dealings entailing data sharing. The personal data protection law should be designated the ruling text entitled to organize and protect all that is related to the circulation of personal data.

- The authorities should revise the procedural rules stated in the personal data protection law. The law should be amended to allow for adding all the regulations related to data protection and sharing, without any reference to executive regulations or administrative decrees. The personal data protection law referred especially important procedural details to its executive regulations. This contradicts the special nature of the law: it is, by its nature, a procedural law. Procedural laws should be comprehensive and self-contained, and all procedural details should be mentioned in it for the sake of stability. Referrals to executive regulations that can be changed single-handedly by the executive authority should be allowed.

- The authorities should abide by the rules provided by the PDPC pertaining to the collection fees in exchange for data protection services. The PDPC service pricing upper limit is very high (EGP 20,000). Hence the PDPC choice of prices should take in consideration the actual cost of data access.

- The ratification of the law should be a step to be followed by the formation of independent agencies capable of following up on the execution of the legal commitments of the law addressees. In this regard, the law's article detailing the composition of the board of PDPC should be amended to allow for the representation of interest groups and data subjects.

- The law should be amended to add clear procedural texts organizing the steps that should be taken in case there is a need to amend, delete, or correct personal data retained by a holder, controller or processor.

- There is a need to amend the law articles pertaining to the role and responsibilities of the PDPC in case there is data sharing across borders. One major responsibility is that the PDPC should explain the dangers entailed in data sharing with certain parties outside Egypt (parties that do not uphold the minimum requirements for data protection). There is also a need to explain the PDPC's role as regards receiving and following up on complaints from users whose data was breached outside the Egyptian borders. And finally, there is a need to clearly state the policies and regulations needed to transfer, store, process, or access personal data across borders, as the law referred this to its executive regulations, which is unimaginable considering the importance of these policies.

- The law's articles pertaining to users' rights should be amended to include committing the controller/processor to provide the personal data requested by the user in suitable format. The data subject also has the right to be informed in case of any violation to his personal data, and hence the law should be clear as regards the time limit for notification and its exact procedures.

- Additional articles obliging the holder/controller to inform the user of his basic rights as regards collecting, processing, retaining, and accessing data should be added to the law. These rights should include informing the user of the aims behind processing his data and giving him the contact information of the holder/controller/processor dealing with it in case he needs to omit or amend something.

https://masaar.net