مؤسسة حرية الفكر والتعبير
Association for Freedom of Thought and Expression

Egypt's Personal Data Protection Law (PDPL) and where it stands according to the international standards

Paper on

Egypt's Personal Data Protection Law (PDPL) and where it stands according to the international standards

Prepared and written by: Alaa Kulaib

A researcher at the Research Unit of the Association for Freedom of Thought and Expression (AFTE)

Publisher:
Association o Freedom of Thought and Expression

info@afteegypt.org
www.afteegypt.org

Content

Methodology

The paper analyzes and studies the Egyptian Personal Data Protection Law (PDPL) No. 151 of 2020 in light of the General Data Protection Regulation (GDPR) of the European Union and *Creating a Data Protection Framework: A Do's and Don'ts Guide for Lawmakers*, a guide issued by Access Now to provide lessons from the GDPR.

The paper aims to provide a preliminary reading of the extent to which the PDPL adopts international standards.

Introduction

Given the spread of daily electronic transactions, the sharing of personal information by individuals with public or private bodies, and the government's plan to shift to electronic transformation instead of paper transactions, the value and importance of protecting digital security has become more evident. Consequently, the defects that may affect this security emerge and create beneficiaries who can unlawfully make use of personal data whether directly or by selling the data to commercial companies and other entities.

On August 18, 2018, President Abdul Fattah al-Sisi ratified the Anti-Cyber and Information Technology Crimes Law (ACITCL). On August 27 of the same year, the Media Regulation Law was ratified, thus legalizing the surveillance of electronic life and restricting digital freedoms[1]. By issuing and ratifying the PDPL in July 2020[2], the Egyptian government sought to accelerate the imposition of its control over the cyberspace and data circulation. But this should have been done in accordance with international standards and the basic rights stipulated in the Egyptian Constitution and law to safeguard the individuals' right to freedom of expression, guarantee personal

1. AFTE, *Statement opposing Egypt's legalization of website blocking and communications surveillance*, September 6, 2018 https://afteegypt.org/en/statements/2018/09/06/15766-afteegypt.html

2. Al-Masry al-Youm, *The Official Gazette publishes the personal Data Protection Law*, a report published on July 17, 2020 https://n9.cl/u7ev

rights and freedoms, and protect personal data from the illegal use by Egyptian authorities.

Accordingly, this paper attempts to provide a preliminary reading of the PDPL and fathom extent to which it is consistent with relevant international standards. This is part of AFTE's interest in protecting and promoting digital rights in Egypt.

The PDPL aims to develop a legislative framework that ensures the protection of users' processed data by safeguarding several subsidiary rights, such as the right to know the nature of the data owned by the entity that holds and processes data. The law also allows the data subject to file a complaint against and sues, if necessary, data users. It also addresses companies and institutions that deal with user databases and, therefore, determines the standards that govern the relationship between users and digital companies. In this sense, the PDPL stipulates the establishment of a digital data protection center to be tasked with overseeing the implementation of the law; issuing licenses, permits and accreditations to companies that process and use individuals' personal data; and providing necessary instructions to guide the law. While we view this as commendable progress that keeps pace with the electronic development of public and private life, the question remains though: Does the law fully preserve digital freedoms? This is what the paper seeks to answer.

Several websites reported that the PDPL modeled relevant international laws, particularly the GDPR[3], with the addition of amendments and standards that contribute to strengthening the protection of personal data. By reviewing a set of international standards for the establishment of a digital data protection law, as well as the abovementioned principles which Access Now[4] considered a benchmark for previous lessons drawn from personal data protection laws, it is possible to measure the effectiveness of the PDPL in protecting users' data while preserving the right to privacy, a right that is primarily associated with personal data. It must be taken into account that this paper provides a preliminary reading of the PDPL until the issuance of its executive regulations.

---

3. Noura Fakhri wrote: *The Personal Data Protection Law for e-shopping; controls you have to know*, published on Al-Youm al-Sabi website on March 16, 2020
https://n9.cl/hhuze

4. Access Now, *Lessons from the EU General Data Protection Regulation*, 2018
https://www.accessnow.org/cms/assets/uploads/2019/11/Data-Protection-Guide-for-Lawmakers-Access-Now.pdf .

First: A look at Egypt's PDPL

The Personal Data Protection Law No. 151 of 2020 consists of 49 articles, divided into 14 chapters and a seven-article preface. Chapter One provides definitions for the terms used by the law, such as "Personal Data", which is defined as "any data related directly or indirectly to an identified or identifiable natural person by connecting such data with other data such as the name, voice, image, etc." It also defines "Sensitive Personal Data" as "data that discloses psychological, mental or physical health; financial data; religious beliefs; or political opinions… children's data is considered sensitive personal data."

Through the rest of the chapters, the PDPL establishes the framework that defines the relationship between the data subject and the data users, including the holder, controller and processor of data, by studying the rights of the data subject, the conditions for data collection and processing, the obligations of the controller and processor, the procedures for making personal data available, the nature of the sensitive personal data usage, cross-border personal data, and the use of personal data in direct e-marketing. From Chapter Nine up to the last chapter, the law provides for the establishment of a Personal Data Protection Center to be tasked with monitoring the enforcement of the PDPL; issuing licenses, permits and approvals for relevant companies; and collecting and processing users' data. It also grants certain individuals from the Center the right to enforce the law. The last chapter is dedicated to crimes and penalties.

Second: International standards, a roadmap to the legislation of personal data protection laws

The right to personal data protection is closely related to the right to digital privacy, which "can be considered as the presumption that individuals should have an area of autonomous development, interaction and liberty, a 'private sphere' with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals", according to the United Nations High Commissioner for Human Rights (UNHCHR) annual report entitled *The right to privacy in the digital age*[5]. The report also covers the individuals' digital life, the area of personal data that falls under the heading of privacy. This was confirmed by Article 12 of the Universal Declaration of Human Rights[6] and Article 17 of the International Covenant on Civil and Political Rights[7].

The UNHCHR report addressed interventions by States and business enterprises that collect personal data of billions of users of electronic transactions, as well as data brokers who trade in personal data of individuals, who find themselves in a situation where it is impossible to trace the path of their personal data and the path of the data usage, given the superior ability to analyze, record and track data and details of users' daily life that they may not want to disclose.

The UNHCHR report indicated the impact of the new technologies on the promotion of human rights[8], especially those related to society and peaceful protests. It also highlighted the need for democratic societies to strengthen the principle of protecting personal data, especially that of individuals who have political orientations. That is

---

5. Human Rights Council, 39th session, *The right to privacy in the digital age; Report of the United Nations High Commissioner for Human Rights*, August 3, 2018
https://undocs.org/A/HRC/39/29

6. Universal Declaration of Human Rights
https://www.ohchr.org/en/udhr/documents/udhr_translations/eng.pdf

7. International Covenant on Civil and Political Rights
https://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf

8. UNHCHR annual report, *Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests*, July 3, 2020
https://undocs.org/A/HRC/44/24

because fragile governments track individuals who have political activity, whether by mail, phones or their websites. Thus, the report emphasizes the importance of protecting personal data by law, especially if society wants to preserve its democratic identity.

Moreover, the formulation of personal data protection laws should take as benchmarks international standards, such as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data issued by Organization for Economic Co-operation and Development (OECD), and the GDPR. The latter has finally become a reference to the formulation of personal data protection laws.

The GDPR aims to codify the process of using individuals' data by large companies or the enterprises that hold or analyze the individuals' data, by setting up the legal framework that establishes and protects that relationship. The GDPR also stipulates the existence of an independent authority that oversees the proper implementation of mechanisms, and seeks to develop the protection of individuals' data as well as the right to privacy in light of the free movement of data.

The GDPR consists of 99 articles divided into 11 chapters, including general definitions and provisions, principles relating to the processing of personal data, the rights of the data subject, and personal data transfer to third countries or international organizations. From Chapter 6 to the end, the GDPR provides for the presence of independent authorities to supervise the legal process, taking into consideration the inclusion of remedies and liabilities, as well as mechanisms for imposing fines in the event of violations.

Unlike the PDPL that applies to individuals and companies, the GDPR focuses on the companies that process users' personal data for different purposes, since it is not concerned with people, but rather seeks to legalize the work of companies. Despite their different preambles, the PDPL and GDPR view political opinions, mental health and children's data with a higher degree of privacy, with the former classifying such data as sensitive personal data and the latter prohibiting the processing or storing of

such data. Both affirm that companies shall not acquire user data[9] without the prior consent of the data subject, granting the data subject the right to review the personal data acquired by companies and the right to modify the data or cancel the contract with those companies. The GDPR also emphasizes some subsidiary rights that guarantee the protection of personal data, such as the right to privacy, the right to erasure ('right to be forgotten'), the right to rectification, the right to be informed, the right to privacy by design and by default, the right of access and transfer of data.

9. GDPR, Definitions
https://gdpr-info.eu/art-4-gdpr/

Third: PDPL under the microscope of international standards

Access Now, one of the associations that were involved in the civil dialogue for the issuance of the GDPR, provided a guideline including the basic principles that the legislator can take into account to formulate a law for protecting personal data and regulating the processing process between different parties. The guide also stated what should be avoided in order not to repeat the same errors of previous experiments. Of those basic criteria:

1. Ensure transparent, inclusive negotiations

This principle is intended to involve civil society institutions, private companies and consumer protection societies in the dialogue on drafting the law, by holding public transparent meetings including all stakeholders. These discussions have to be free from any form of pressure and be highly transparent and impartial, a method followed by EU countries in drafting the GDPR.

Conversely, the PDPL ignored this important step and did not involve various groups of society. All that happened was that after 60 lawmakers had submitted the draft law, the Minister of Communications and Technology announced the government's approval of the bill in 2019 and the House of Representatives (parliament) finally approved it[10]. The legislature's failure to involve various society groups in the drafting and preparation of the PDPL suggested that the law could possibly include deficiencies in its objectives.

2. Define and include a list of binding data protection principles in the law

According to this principle, the law must include clear concepts of personal data and sensitive personal data, as well as the applied procedures for personal data during the communications to preserve the privacy of these communications and the privacy of

10. Abdullah Magdy wrote: *A three-thousand-year idea; details of the Personal Data Protection Law*, published on Masrawy website on July 18, 2020
https://www.elwatannews.com/news/details/4908354

the data exchanged as well. This principle ensures that the law includes the Eight Data Protection Principles, Convention 108, and OECD Guidelines[11] - namely collection limitation principle, purpose specification principle, use limitation principle, data quality principle, limitation of data retention period, rights of users including the right of access to data and the right to erasure, integrity and confidentiality, and finally, compatibility in data transfer to another country or territory that has an adequate level of protection.

The PDPL provided clear definitions for personal data, sensitive personal data, as well as the holder and processor of data[12]. It sought to preserve the right of the data subject, whether the processor is an individual or a company, by criminalizing the use of data without the knowledge of its owner or by refusing to enable the data owner from having access to their data. However, State agencies are excluded from this criminalization and the law did not define their work tasks, by excluding security bodies and the databases controlled by the Central Bank and its affiliated institutions from being subject to the provisions of the PDPL.

3. Define legal basis authorizing data to be processed

This principle stipulates that the law shall define the legal basis under which any entity that processes data must comply with the law by implementing the terms of the contract with the user's consent and in all the user's rights. This means the user has the right to give or withdraw their consent. This is what the law guarantees in Article 2, which is "the right to withdraw prior consent to retain or process personal data".

11. Organization for Economic Cooperation and Development, *Guidelines governing the protection of privacy and transborder flows of personal data*, 1980
https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/OECD_Privacy_Guidelines_1980.pdf

12. Personal data as defined by law is "any data relating to an identified or identifiable natural person directly or indirectly by associating such data with any other data via name, voice, image, identification number, online identifier, or any data identifying psychological, health, economic, cultural or social identity."
Sensitive data: "Data that discloses psychological, mental, physical or genetic health, biometric data, financial data, religious beliefs, political opinions, or security status. In all cases, children's data is considered sensitive personal data."

4. Include a list of binding users' rights in the law

This principle guarantees users to control their data in accordance with basic rights, which the law must define, namely the right to object, the right to erasure, the right to rectification, the right to information and the right to explanation. The law guarantees all these rights. However, it sets financial consideration of no more than 20,000 ($1,273) for the exercise of those rights, except for the right to information in the event of a violation of personal data. The Data Protection Center issues decisions related to determining and receiving the financial consideration.

5. Define a clear scope of application

Violations relating to digital rights and protection of personal data go beyond the traditional form of many crimes that are limited by place and time and mostly take place within the geographical territory on which the State has sovereignty. Conversely, a problem arises when formulating personal data protection laws around the world. Some expand the scope of the application to include any individual or entity on the State territory, as well as any entity anywhere else in the world whether belongs to the State or processes the data of its citizens. But in this particular case, more complications and potential conflict of laws arise. So, it is important to take them into consideration when drafting laws.

Article Two of the PDPL clarifies the scope of its application to include anyone who commits one of the stipulated crimes as long as the offender is "an Egyptian residing inside or outside the State, a non-Egyptian residing inside the State, or a non-Egyptian residing outside the State, if the act is punishable in the country where it occurred under any legal designation and the data of the crime belong to Egyptians or foreigners residing inside the State"[13] .

6. Create binding and transparent mechanisms for secure data transfer to third countries

Under the GDPR, cross-border data transfer may only take place with a third country that has been accorded an adequacy status, which is determined by a decision of the EU

13. Article 2 of the Personal Data Protection Law No. 151 of 2020

Commission to ensure that the State has an adequate level of protection by reason of its domestic law or its international commitments. The EU Commission has the power to determine whether a third country has an adequacy status or not. Many countries seek to obtain this decision. This principle provides for not circulating personal data with a third country through space agencies or others unless this country has an adequacy status. The law must stipulate the procedures of data transfer to third countries.

The PDPL warns against cross-border data transfer, whether through collection, storage, processing or sharing with a foreign country that has a level of protection lower than that stipulated in the law. Data transfer may only be carried out with a license from the Data Protection Center. However, the PDPL left the matter of determining policies, standards, procedures and rules to the executive regulations. The law does not mention anything similar to the adequacy status, neither.

7. Protect data security and data integrity

The PDPL guarantees the confidence of users through the presence of a large number of liabilities for the parties responsible for collecting, modifying and processing data. The law provides for many forms of penalties in the event of any abuse by those parties or persons concerned. The law also guarantees the protection of users' data without exposing them to any form of danger.

The PDPL states that in the event that the Data Protection Center employees are proven to have committed a crime violating the provisions of the law, the Minister of Justice shall issue a decision based on the proposal of the minister authorized to enforce the law.

However, the PDPL does not address cases of peaceful demonstrations in light of technology and electronic surveillance. The law does not address the protection of personal data for those who have opposition political views or held political positions in the past. Nor does it address cases of peaceful demonstration, protection of protesters' data from mass surveillance, and protection of demonstrators. Despite the inclusion of political opinions within the sensitive data, the exclusion of security agencies from the law is a major loophole that undermines the value of sensitive data.

8. Develop data breach prevention and notification mechanisms

This principle encourages the spirit of continuous development to adopt mechanisms capable of protecting data and preventing breaches. This can be achieved by keeping pace with technological developments and seeking assistance of communication, data and technology experts to develop mechanisms for electronic work.

The PDPL, at the beginning, defines breach of personal data and breach of data[14] and grants the data subject the right to information in the event of any breach or violation of their data and the right to resort to the judiciary in the event of any breach of their right to protection of personal data. The law also obliges the data processor or controller to notify the Center within 72 hours in the event of a breach or violation of personal data. Notification shall be made immediately if the data affects national security. The Center shall, within 72 hours from the date of its knowledge, define the nature and form of the reasons for the breach, and identify potential effects and the measures to be taken. The Center shall, in turn, notify the data subject of that incident within 72 hours from the date of reporting.

The law's executive regulations determine the procedures for reporting and notification. But it does not specifically mention any kind of technological developments that need preparations for developing mechanisms to face up to the violation and breach.

9. Establish independent authority and robust mechanisms for enforcement

This principle emphasizes the need for an independent authority to oversee the law enforcement in a strict manner and impose fines on companies, especially small and medium-sized enterprises that may not adequately comply with the law during the processing of personal data as stipulated in the law and international standards.

The PDPL stipulates the establishment of a Data Protection Center, which, according to the law, has the power to set and implement policies, strategic plans and data protection programs. The Center also has the right to set measures; define procedures;

14. The law defines breach and violation of personal data as: "Every unauthorized entry or unlawful access to personal data, or any unlawful operation of copying, sending, distributing, exchanging, transferring or circulating with the aim of revealing, damaging, modifying during storage, transferring or processing personal data."

coordinate and cooperate with governmental and non-governmental agencies and related initiatives; issue licenses, permits and approvals; receive complaints and reports; express an opinion on draft laws and international agreements that regulate the development of personal data protection; monitor the procedures stipulated by law; verify the conditions for cross-border data transfer; and take related decisions.

The Board of Directors consists of 10 individuals, who are representatives of the Ministry of Defense, Ministry of Interior, General Intelligence Service, Administrative Control Authority, Information Technology Industry Development Authority, National Telecommunications Regulatory Authority, the Center's CEO, and three experienced persons. The structure of the Board of Directors cannot be overlooked, as seven members belong to government bodies and three others represent security agencies, which are already excluded from the law. This gives these agencies the right to acquire databases without oversight or legal restriction.

The legislator also placed security agencies as a primary destination for the data processing operations and checking violations, making them a reference to the Center. The law also obligates the person who processes or controls data to immediately inform the security authorities within 24 hours.

Thus, the Data Protection Center loses its independence by being almost fully affiliated with government agencies, not to mention the absence of any representatives from civil society and the unlimited powers granted to security services.

10. Continue protecting data protection and privacy

There is a global trend to ensure the protection of the right to privacy in constitutions. This may take such a classic form as Article 57 of the Egyptian Constitution which states that private life is inviolable and safeguarded. It may be formulated in modern terms that explicitly provide for security, digital privacy and personal data.

The issuance of the PDPL is an important step in this context. But the lack of independence on the part of the Center that enforces the law and the exclusion of security authorities from being subject to the law impede the implementation of citizens' rights to privacy and digital security.

Fourth: PDPL vis-à-vis databases maintained by telecommunications companies, practices violating protection of personal data and the right to privacy

The AFTE published a publication entitled *Privacy Policies of Communication Companies in Egypt*[15] that addressed the situation of the four telecom companies and how they seized a giant database of their customers from the moment of signing the contract and providing the company with a copy of the customer's national ID.

The report also indicated that the state-owned Telecom Egypt (We) has not provided any information about the privacy policy either on its website or regarding the telecommunications services it provides. The four telecommunication companies operative in Egypt share user data with third parties, whether for law enforcement, marketing, or debt collection purposes. The four companies receive a huge amount of personal information, without obligations or mechanisms to manage the giant databases they control. Moreover, the two companies Telecom Egypt and Orange condition that users comply with certain rules that restrict the freedom of expression and access to information.

Many practices allow the violation of personal data, including incidents of searching citizens' mobile devices in main squares by security men, especially in the wake of the opposition demonstrations in September 2019. These also included leaking data of survivors[16] of mass harassment and rapes at Tahrir Square on June 3 and 8, 2014 during President Abdul Fattah al-Sisi's swearing-in. ON TV and Al-Youm Al-Sabi newspaper published the personal data and photos of the survivors in flagrant violation of the survivors' rights to privacy and protection of their personal data, putting them at risk and threat.

15. AFTE, *Privacy Policies of Communication Companies in Egypt*, December 30, 2018
https://afteegypt.org/en/digital_freedoms-2/publications_digital_freedoms-digital_freedoms-en/2018/12/10/16654-afteegypt.html

16. Cairo Institute for Human Rights Studies, *Disclosure of Personal Information of the Survivors is a Flagrant Violation of their Privacy and Disregard for their Safety*, June 26, 2016.
https://n9.cl/6u48

Also, those in charge of Sabaya el-Kheir TV program, presented by Reham Saeed, hosted a survivor of a sexual assault that had taken place in a shopping mall. After the survivor recounted the details of the incident, refusing to identify herself, the program's producers revealed the identity of the survivor and showed her photos and some details of her personal life[17]. This caused discontent on social networking sites. Pressures through online campaigns on the program led the management of the channel, Al-Nahar TV, to suspend Sabaya el-Kheir and opened an investigation into the accusations attributed to the program. The channel also deleted the survivor's video from YouTube.

17. AFTE, *When privacy and press freedom clash: The case of anchorwoman Reham Saeed*, November 2, 2015 https://n9.cl/vmw4k

Conclusion and recommendations

The issuance of the PDPL represents an attempt by the authorities to keep pace with the developments and protect the right to privacy, which overlaps with the protection of personal data. However, the law implies shortcomings represented in the absence of societal debate and transparency in issuing the law, as well as the lack of independence of the law enforcement center. The shortcomings can be addressed in the executive regulations. We hope the authorities will be highly aware of and responsive to the developments taking place in the electronic world in a way that protects and enhances both the digital and physical human rights, instead of violating or allowing the violation of such rights.

If this is not possible through the executive regulations, there will be a need to amending some provisions of the law. For example, there is a need for the provision of material exemption from exercising basic rights related to data protection - that's, users should not have to pay for exercising their right to know the data used by the entities that process and analyze their data. Also, there remained a need for State agencies to reduce their authority over controling database mechanisms. A competent, independent and transparent oversight authority is also required. A wider space for the involvement of various groups in the drafting of the executive regulations is needed as long as no opportunity was available during the law drafting. We also hope the regulations will define the term "private life is inviable", which is stated in the law without giving further details to explain it, so that we should not find vague terms that may have more than one meaning.