Data Protection in Egypt

The Present and the Future

Mohamed Hemdani

Acknowledgments to Chevening Scholarships, the UK government's global scholarship programme, funded by the Foreign and Commonwealth Office (FCO) and partner organisations.

Table of Contents

Conclusion

Introduction

As it heads towards stability after a rough period of uncertainty and political turbulences, Egypt is now trying to be an investment appealing market, and realizing that data is an important aspect of business and security, especially in the highly expanding online life, the Egyptian legislature is now in process of adopting necessary laws to maintain data safety in order to boost the trust in all aspects of electronic transactions, occurring within the Egyptian territories in addition to maintaining national security.

And as data is increasingly becoming the new valuable currency, the huge range of usages of data that is beeing collected from different sources, known as "Big Data", has been the center of attention for both businesses and governments.

Data now stream from daily life: from phones and credit cards and televisions and computers; from the infrastructure of cities; from sensor-equipped buildings, trains, buses, planes, bridges, and factories. The data flow so fast that the total accumulation of the past two years—a zettabyte—dwarfs the prior record of human civilization. "There is a big data revolution," says Weatherhead University Professor Gary King. But it is not the *quantity* of data that is revolutionary. "The big data revolution is that now we can *do* something with the data."[1]

In marketing, familiar uses of big data include "recommendation engines" like those used by companies such as Netflix and Amazon to make purchase suggestions based on the prior interests of one customer as compared to millions of others. Target famously (or infamously) used an algorithm to detect when women were pregnant by tracking purchases of items such as unscented lotions—and offered special discounts and coupons to those valuable patrons.

Credit-card companies have found unusual associations in the course of mining data to evaluate the risk of default: people who buy anti-scuff pads for their furniture, for example, are highly likely to make their payments.

It's been anticipated that revenue from big-data-related hardware and software products and services is to exceed $50 billion by 2017.[2]

---

[1] Jonathan Shaw, Why "Big Data" Is a Big Deal, < http://harvardmagazine.com/2014/03/why-big-data-is-a-big-deal> accessed 11/2/2016

[2] Rick Whiting, 2015 Big Data 100: Business Analytics, < http://www.crn.com/slide-shows/data-center/300076704/2015-big-data-100-business-analytics.htm?itc=refresh> accessed 24/7/2016

In the public realm, there are all kinds of applications: allocating police resources by predicting where and when crimes are most likely to occur; finding associations between air quality and health; or using genomic analysis to speed the breeding of crops like rice for drought resistance. [3]

Being a valuable currency, data needs protection, the ways data is being collected, processed and used, raises a lot of legal concerns most importantly, about privacy. Furthermore protecting data will definitely lead to economic flourish as data subjects trust the safety of their data from various kinds of violations making them more willing to provide it and consent to process it as long as they are sure it's not going to be misused.

The increasing use of the internet in Egypt makes Egyptians a very valuable data subjects for different kinds of beneficiaries, basically, data analysis businesses and, in a lot of cases, the government.

Looking at the latest trends related to Facebook and Twitter in the region, we can find that over 9.3 million users from Egypt alone are on Facebook, with over 1.214 million on Twitter. Egypt is the largest population online when compared to other MENA countries[4].

Unfortunately, Egyptian users are vulnerable to all types of cyberattacks due to poor security awareness and education programs with absence of "privacy and cyber legislation".
Most Middle East and North African countries, including Egypt, have ranked high in financial crimes such as fraud, bribery, corruption, and money laundering. That makes the region a suitable environment for "Financial Cybercrime".[5]

Today's cybercrime costs the economy $388 billion, Symantec revealed. This shocking statistics is made up of two parts: $274 billion, Symantec's estimate of the value of time lost to cybercrime in the past year; added to $114 billion, said to be the industry's "direct cash costs." That is, the amount of money "spent on resolving cyber-attacks" and the amount of money directly stolen by cybercriminals.[6]

The 2012 report published by APWG revealed that Egypt has ranked in the top three countries for hosting phishing websites.[7]

Realizing the importance of data protection and cyber security, the Egyptian constitution 2014 contained 2 provisions regarding this matter.

---

[3] Ibid1

[4] http://www.guardian.co.uk/world/2012/jan/26/african-twitter-map-continent-connected accessed 15/8/2016

[5] http://www.pwc.com accessed 15/8/2016

[6] Mohamed N.Elguindy, Faisal Hegazy, Cybercrime legislation in the middle east, information systems security association, Published February 27, 2012
https://www.researchgate.net/publication/259583247_Cybercrime_Legislation_in_the_Middle_East accessed 15/8/2016

[7] http://www.antiphishing.org in Ibid page11

Article 31 of the constitution provides that "The security of information space is an integral part of the system of national economy and security. The state commits to taking the necessary measures to preserve it in the manner organized by law"

Article 57 of the Egyptian Constitution 2014 provides for the protection of privacy and secrecy of, inter alia, mails, phone conversations and other methods of communication. The aforementioned shall not be monitored, inspected or confiscated unless by virtue of a prior court order and for a limited period of time as regulated by the law.

Until this moment, Egypt does not have a law which regulates the protection of personal data. However, there are some piecemeal provisions in connection with data protection in different laws and regulations in Egypt.

For example, the Egyptian Penal Code no. 58/1937 imposes criminal punishment for unlawful collection of images or recordings for individuals in private places. Some other laws provide for protection and confidentiality on certain data, such as the Egyptian Labor Law no. 12/2003 (confidentiality of the employee's file information including punishment and assessment) and the Egyptian Banking Law no. 88/2003 (confidentiality of client and account information). Egyptian

Civil Status Law no. 143/1994 provides for the confidentiality of citizens' civil status data. The Executive Regulations of Mortgage Finance Law no. 148/2001 issued by virtue of Cabinet Decree no. 1/2001 as amended by Prime Minister

Decree no. 465/2005 has a similar clause which provides for the confidentiality of the data of the clients of mortgage finance companies. The Egyptian Telecommunications Law no. 10/2003 provides for the privacy of telecommunications and imposes penalties which account to imprisonment in some cases on the unauthorized violation of such privacy.

Article 16 of the Egyptian Antitrust law also provides for an obligation for confidentiality on officials of the antitrust authority for the data collected related to their work and article 23 makes it a misdemeanor.

A similar article exists in the consumer protection act, article no. 18, while article 24 thereof makes it a misdemeanor.

Article 21 of the electronic signature act provides for a similar provision as well.

Article 97 of the Egyptian banking law notes the confidentiality of client and account information.

However, are those laws enough for providing protection to data and do they satisfy the purposes of articles 31 and 57 of the constitution? And if the answer is no, how can the Egyptian legislature find a way to better protect data, and consequently boost the Egyptian economy and national security?

In this paper I will try to shed some light on the current situation of data protection in Egypt and then move on to the ongoing discussions about the proposed law concerning this matter, and how

this might be a significant change in the data protection and privacy protection policy in Egypt by clarifying the way it deals with the threats imposed on data and privacy, and the motives behind adopting this law now and what possible enhancements could be made to make the proposed law more practical and goal achieving.

I will start with a relatively detailed overview of the laws currently containing provisions for data protection, then will have an overlook on the proposed law with an in depth look at the provisions dealing with protection of data from various sorts of violations.

** For the purposes of this paper, the proposal of the law was used to make the analysis and used as a reference for article numbers and content, no definite legislation was adopted until this moment, and consequently none of the information regarding the articles of the proposed law should be deemed official or final.

Chapter 1

A- Current situation of data protection in Egypt

As a Muslim country, Egypt is keen on drafting most of its laws in conformity with the Islamic Sharia especially that Sharia principles are the main source of legislation[8] as provided for in the constitution.

Protection of privacy is a fundamental right according to the principles of Islam. In Quran, Allah says "**O you who have believed, avoid much [negative] assumption. Indeed, some assumption is sin. And do not spy or backbite each other.** "[9], that is considered a direct order not to spy for the protection of people's privacy.

Furthermore, a lot of Prophet Muhammad's (PBUH) sayings (Hadith) are related to the respect of privacy as he said **"Avoid suspicion, for suspicion is the gravest lie in talk and do not be inquisitive about one another and do not spy upon one another and do not feel envy with the other, and nurse no malice, and nurse no aversion and hostility against one another and be fellow-brothers and servants of Allah"[10]**.

Despite the inherent importance of the right to privacy, until the time of the writing of this paper, no actual law concerning the protection of data and privacy has been adopted in Egypt, only scattered provisions in different laws in addition to the constitution, that's why the Egyptian legislator was motivated to adopt a law especially concerned with data protection.

---

[8] Article 2 of the Egyptian constitution states that "Islam is the religion of the state and Arabic is its official language. The principles of Islamic Sharia are the principle source of legislation."

[9] Quran, Surah "Al Hujurat", verse no.12

[10] Muslim Book 32, Number 6214, http://fatwa.islamweb.net/fatwa/index.php?page=showfatwa&Option=FatwaId&Id=45328 accessed 29/7/2016

In order to get a full picture of the motives behind the proposed laws, we will go through the different provisions in the Egyptian law concerning the protection of data and privacy to further know why it is crucial to have a data protection law.

I- Constitutional protection of data and privacy

Article 57 of the current constitution deals with the right of people to privacy in various ways as it provides that "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."[11]

This principle was emphasized by many of the Egyptian constitutional court decisions, that signified that there are areas of everyone's lives that should not be accessible to anyone for the sake of protection of his private life, especially using recent technology that made it easy to access such areas, thus protecting individual's right to privacy also protects his right to make decisions with free will.[12]

Article 31 of the constitution provides that "The security of information space is an integral part of the system of national economy and security. The state commits to taking the necessary measures to preserve it in the manner organized by law"

That is another very important aspect of data protection, the protection of information on the internet and considering it as a matter of national and economic security.

So, despite the right to access to public information provided for in article 68 of the constitution[13], the right of people to privacy and the protection of their personal data are protected by articles 31 and 57.

II- Data protection in the Telecommunication Act no. 10/2003

The main purpose of the Telecommunication Act is to create a legal framework for the regulation of communication networks and services, which aims at securing the optimum usage of frequency spectrum, guaranteeing the provision of communication services to all regions across the country, including remote areas,, safeguarding confidentiality of telecommunications, and seting up a regulatory authority for the sector of communications[14].

---

[11] Art.57 Egyptian Constitution 2014

[12] Case no.23 of the year 16 constitutional, 18/3/1995.

[13] Article 68 of the Egyptian constitution 2014 provides that "Information, data, statistics and official documents are owned by the people. Disclosure thereof from various sources is a right guaranteed by the state to all citizens."

[14] Egypt: Telecommunication Regulation Law, https://www.article19.org/data/files/medialibrary/37966/Egypt-telecoms-report---English.pdf data protection in egypt accessed 30/7/2016

The act's main accomplishment was establishing NTRA "National Telecommunication Regulatory Authority" and the Egyptian Company for Telecommunication (Telecom Egypt).

NTRA has a public juristic personality and subordinate to the minister of communications and is entitled to manage communications in the country.[15]NTRA also issued the first license to a telecommunications company to Telecom Egypt according to the law.[16]

The act has three main provisions regarding data management and privacy. Article 19 provides for an obligation on all companies working in the telecommunication field to provide NTRA with any information except for national security related matters.

This law is considered to be the closest legislation to a specified law dealing with protection of data in the field of communications. A first concern about this law would be the non-independence of NTRA from the control of the government as art.3 provides for its sub ordinance to the Minister of Telecommunications.

That is one aspect that should be effectively enhanced, by omitting the subordination of NTRA to the Minister, and by changing the way its members are appointed, as most of them are appointed by the government represented in the Minister of Telecommunications.[17] Thus increasing the members appointed by Civil Society Organizations and non-governmental bodies and the existence of judicial representation shall definitely increase the autonomy of NTRA, we will see later how did the proposed law dealt with the formation of a similar authority.

Preserving national security is evidently a main concern to the legislator drafting this act, which is shown in the drafting of article 64, giving a lot of powers of disclosure to the Armed Forces and investigation authorities. Despite the importance of that, some people see this article as vague and gives wide powers to the investigation authorities[18], however, this argument is not correct, as the article itself restrained the powers given to the authorities to disclose information, when providing that the exercise of those powers shall give "*consideration to inviolability of citizens private life as protected by law*", making it an obligation to respect the procedures provided for in the Criminal Procedural Law for getting or disclosing any information.

In article 71, the legislator provides that it shall be a misdemeanor punishable by imprisonment and/or fine if any person, while performing his duties in the field of communications disclosed any information.

It is notable here that the law does not describe a specific definition of data or information nor distinguish between personal data and other types of data, however it uses the term "information" as mentioned in article 71, which might cause some problems in terms of application if we tried to extend the application of such provisions beyond the telecommunication services as defined by the

[15] Art.3, Egyptian telecommunications act no.10 of 2003
[16] Ibid, art.60
[17]Ibid15, Article 12

[18] Ibid14, page13

law[19] to encompass all kinds of services performed online where "data controllers" have access to a lot of data concerning their clients.

Generally, the law did the job until this point in the field of telecommunications, however recent developments in the field of information technology and the internet specially in the last ten years makes the law's ability to cope with new developments and challenges questionable, thus in addition to not having a lot of necessary definitions, the law lacks provisions criminalizing various sorts of breaches to privacy and information security.

III- Data protection in Law no.3 of 2005 on the Protection of Competition and the Prohibition of Monopolistic Practices

This law was drafted with the aim to promoting a competition culture and tackling anti-competitive behavior in the Egyptian market.

Data is a very valuable tool in maintaining competitiveness in the market, the collection and exploitation of data may raise barriers to entry and be a source of market power. It may also reinforce market transparency, which may impact the functioning of the market. There are several types of data-related conducts of an undertaking that might raise competition concerns[20].

Therefore, the protection of certain kind of data is crucial in ensuring stability to the market and consequently important to the economic wellbeing.

The Egyptian legislator was alert to this fact, establishing in article 16 an important obligation on the employees of the Authority for the Protection of Competition and the Prohibition of Monopolistic Practices to disclose any information or data or sources in relation to cases under the scope of the law limiting the use of those data to the purposes for which they were submitted.

Article 23 of the law punishes the breach of the provisions of Article 16 of this Law by a fine not less than ten-thousands Egyptian Pounds and not exceeding fifty-thousands Egyptian Pounds.

There is no doubt that this is one of the most important provisions of the law, however, it also lacks definitions of data and information despite the use of both terms in article 16, in addition to the lack of a provision stipulating the form those information or data might take, opening the door to narrow explanations that might exclude some sorts of data consequently resulting in their divulgence without being able to punish whoever was responsible for such divulgence.

IV- Data protection in Egyptian Penal Code

The Egyptian Penal Code is the code dealing generally with crimes and punishments, regardless to other punishment provisions existing in other special laws.

Article 309 bis, providing for the penalty of imprisonment not exceeding one year for eavesdropping, recording, transmission of talks taking place in private places or via telephones, in addition to shooting, taking or transmission of photos of a person in a private place. A sole

[19] Ibid15 art.1 para 7, provides that "Telecommunication Service Provider: Any individual or juristic person authorized by the NTRA to provide one or more of the Telecommunication Services."

[20] Competition law and data www.autoritedelaconcurrence.fr/doc/report**competitionlaw**and**data**final.pdf page 11

exception to this provision is the presumable consent of the person if that happens "before the eyes and ears of the attendees". The punishment is intensified on a public servant committing this crime to imprisonment.

Another related article is article 309 bis A, provides for a punishment of imprisonment of maximum five years for the disclosure, use and divulgence of the documents obtained by the methods provided for in the previous article. While the punishment of the unlimited imprisonment is provided for the public servant committing this crime.

While article 310 protects the secrets held by "physicians, surgeons, pharmacists, midwives, or others whom a secret is deposited by dint of his profession or position" from being disclosed, providing a penalty of imprisonment not exceeding six months or a fine not exceeding 500 EGP.

What is to be noticed here is the general exception of consent to disclose such information, a notion that has been signified by many decisions of the court of the Egyptian court of cassation.[21]

V- Procedural protection of data and privacy

Investigatory powers regarding disclosure of data and breach of privacy has always been a controversial matter. While maintaining security is an important objective of every government, sometimes it's hard to do this while preserving the people's right to privacy.

In Egypt, the law that gives investigatory authorities the right to disclose information and breach a person's privacy is basically the Criminal Procedural law.

Article 95 of the law gives the "investigating judge" the authority to seize letters, telegrams and any other printed papers or packages at the post, in addition to tapping calls as long as this is beneficial in detecting a crime punishable with at least 3 months in imprisonment.

Judge's order should be sufficiently reasoned for a maximum period of 30 days extendable to a similar period.

The reasoning of the judge order for seizure or tapping phone calls is a very important guarantee, as the Egyptian court of cassation affirmed in a lot of decisions that if the judge's order is not sufficiently reasoned; the judge has not made sure that his order was issued based on sufficient investigations, would render such order void, consequently voiding all consequent evidence.[22]

An exception to this article is article 96 which provides that the judge shall not issue an order of seizure to any documents delivered by the suspect to one of his lawyers or to an expert.

Another exception is the authority of the public prosecutor, not a judge, to assume the same authorities of the investigating judge in the crimes that constitutes a threat to the national security as defined in the Penal Code.

The later principal was affirmed by a lot of decisions of the Egyptian court of cassation.[23]

---

[21] Case no. 1832, judicial year no. 10, dated 9/12/1940.

[22] Case no.8792, cassation year 72, session date 25/9/2002

[23] Case no. 50614, cassation year 74 session date 7/12/2005

The above mentioned provisions put some restrains on the government – vested in the investigation authorities - ability of surveillance over persons, however, the tight wording of those provisions makes them too outdated to cope up with the huge leap in technology and communications leaving a big gap between what is written in the law and real life, which makes sense given that this law was drafted in 1950, and it's last amendment was in 2003.

VI- Data protection and the Electronic Signature Law

The main purpose of the E-signature Law was to give the value of proof to the electronic signature, in addition to establishing Information Technology Industry Development Authority (ITIDA), with the aim of, inter alia, encouraging and developing information and communications technology, and encouraging and developing investments in information and communications technology industry.[24]

In addition, and for the first time, a set of comprehensive definitions concerning electronic signature and most importantly, the electronic document and electronic writing were provided for in the Law.[25]

Article 21 of the law provides for the confidentiality of e-signature and e-media data and information submitted to the entity licensed to issue digital certificates, article 23 sets a penalty of imprisonment and a fine of 10000 to 100000 EGP or either, for obtaining unrightfully a signature, written message or electronic medium; or breaching, intercepting or putting such electronic media out of service.

Definitions play a huge role in data protection in this Law, and they also reflect on the protection of data in general, even in other laws, definitions provided for in the Law for electronic writing and electronic document[26], widens the scope of protection on any document originally created in an electronic form or transferred to an electronic form. Thus article 15 gives electronic writing and electronic documents the same legal effect of their paper counterparts.

Consequently, the protection provided for in the Criminal Procedural law, article 95 and 96 previously discussed, is now extended to all sorts of documents including electronic ones, making it forbidden for investigation authorities to hack to someone's email, for example, unless they have a properly reasoned order from the investigating judge.

However, a full protection of all sorts of communications and online data transactions still has no definite frame in the Egyptian law until this point.

VII- Data protection in The Law of The Central Bank, The Banking Sector And Money

This Law is basically responsible for regulating banking sector, a very important part in the economy of any country.

---

[24] Art.3 Egyptian e-signature law no. 15/2004

[25] Ibid, art.1

[26] Ibid art. 1/a,b

Protection of data of bank clients is a key element of trust between that bank and the client, thus reducing market confidence in transactions like online banking.

That is why a whole section in the law was dedicated to maintaining the Secrecy of Accounts[27], articles 97 to 101. These articles set the principle of secrecy of all accounts, deposits, trusts, and safes of customers at banks, as well as their related dealings, in addition to an obligation of non-disclosure on the board chairmen and members of banks, real estate finance companies, financial lease companies, inquiry and credit rating companies, as well as their directors or staff of the previous information.

The protection of data in this law does not stop at people dealing directly or indirectly with these data, it extends to investigating authorities powers with an exceptionally complicated procedure of disclosure. Article 98 of the law provides for disclosure or access to the information in article 97 only by virtue of a court order from Cairo Court of Appeal, to be issued upon request from the Attorney General or any one he delegates from among at least the first public attorneys, or upon the request of an official or interested party.

Such relatively long process ensures that disclosure of such delectate information is only done when it is really necessary. One exception of the above mentioned mechanism is the authority of the Attorney General or whoever he delegates' from among first attorneys to disclose these information in the course of investigating a crime related to public domain and money laundering crimes.

Article 124 punishes the violation of articles 97 to 100 with imprisonment for a period of not less than one year, and a fine of not less than twenty thousand pounds, and not more than fifty thousand pounds. While article 125 punishes whoever among the workers in charge of enforcing the provisions of this Law divulges any data or information he has ex officio obtained with imprisonment for a period not exceeding two years, and a fine of not less than five thousand pounds, and not exceeding ten thousand pounds or either penalties.

In this law, the legislature tried to protect all sorts of data gathered or processed by financial services institutions. However it did not contain specific provisions for the protection against technology related breaches for client data like card frauds schemes and identity theft crimes.

It is worth mentioning here that the central bank of Egypt is entitled to update banks with security measures regarding clients data with periodic instructions of his powers derived from article 6 of the law.

VIII- Data protection in the Civil Status Law

The Civil Status Law is the law regulating registration of births, deaths and issuance and management of national identification numbers with all associated information about citizens.

[27] Section 4 , law no. 88 of the year 2003 Promulgating The Law of The Central Bank, The Banking Sector and Money

Article 13 of the law provides for the secrecy of all the registered information concerning the citizen's civil status, what is more, it is considered a "national secret" that cannot be disclosed without a written permission from the head of the civil status authority.

The same article regulates the way of disclosure of such information by the judicial authorities or the public prosecution and it obliges the judge or the investigator "the public prosecutor" to physically move to the authority's headquarter examine those information.

Section nine of the law titled "Guarantees of the Protection of Citizens' Rights" consists of two articles (64, 65). Article 64 provides for the way information is being collected from the citizens and that such information should not contain anything about political tendencies or beliefs or the criminal records unless otherwise provided for in the law.

On the other hand, article 65 provides that the civil status authority is committed to take all necessary measures to secure personal data collected and stored on computers or the attached storage media against any breach or manipulation or access disclosure or destroy unless otherwise provided for in the law according to the procedures provided for therein.

Article 74 sets a punishment of imprisonment of not less than six months and a fine not less than 500 pounds or either for whoever accesses or attempts to access or acquire or attempt to acquire any of the information or the data in the registers or computers or the attached storage media or alter it in any way, the penalty becomes the imprisonment of the culprit if the criminalized act occurred on the collective data or information or statistics.

Overall, in terms of data protection in this law, the articles that dealt with it is sufficiently protective, however, the lack of accurate definitions for some of the terminology used in the law such as "personal data" and the difference between "data" and "information" adds uncertainty to the accurate meaning of the articles dealing with data and information protection.

IX- Egypt and the international efforts in the field of data protection

In a study conducted by the United Nations Office on Drugs and Crime "UNODC"[28], it was found that more than half of responding countries to the survey conducted in relation to the study, reported that between 50 and 100 per cent of cybercrime acts encountered by police involved a 'transnational element.' The prosecution of transnational acts requires states to assert two types of 'jurisdiction' – both substantive and investigative.

Furthermore, studies shows the global cost of cybercrime is estimated to be between $375 billion and $575 billion annually'-greater than the 2013 Gross Domestic Product of all but thirty of the world's countries[29], making combating cybercrime is a matter of international importance on both economic and security level, a matter that requires solidarity and cooperation on the international level.

---

[28] Comprehensive study on Cybercrime, draft February 2013, United Nations, New York 2013.

[29] Patrick Stewart, TRADING CYBERCRIME FOR JOBS AND COMMERCE OR PAYING UP: USING THE WTO TO COMBAT CYBERCRIME, 48 Geo. Wash. Int'l L. Rev. 475 2015-2016

Consequently, countries should adapt their laws in a way accepting their application to an act that takes place only partly, or even not at all, within its national territory. In addition, states need to be able to carry out investigative actions that concern the territory of other states. It has to be acceptable that investigations may involve infringements on the sovereignty of states, so, formal and informal processes of consent and international cooperation are required. Many of these are at the level of international treaty law, both multilateral and bilateral. National laws, however, can also specify procedures to be applied, or create bases for cooperation in their own right.[30]

Recognizing that, and acknowledging the importance of international cooperation in the field of data protection and cybersecurity, that international cooperation in the field of data protection has always been the key tool in combating cybercrime, especially that cybercrime is known of its interregional nature and the constant existence of transitional elements[31], Egypt has joined the League of Arab States Convention for Combating Information Technology Crimes (Arab Convention).

The purpose of this Convention as mentioned in its preamble, is to enhance and strengthen cooperation between the Arab States in the area of combating information technology offences to ward off the threats of such crimes in order to protect the security and interests of the Arab States and the safety of their communities and individuals.[32]

The basic structure of the Convention consists of five chapters, the first chapter is general provisions which basically deals with necessary definitions and the scope of application, second chapter deals with relatively detailed definitions for various kinds of information technology related crimes, while the third chapter contains the procedural provisions which are in essence answering the question of how the member states would implement this conventions and integrate it in their legal systems, while chapter four is about legal and judicial cooperation and the fifth chapter is for about final provisions regarding ratification and limitations to the application of the treaty.

The first remark concerning Egypt with regards to that convention is the delay of the date of the coming into force of the convention, the convention was signed in 2010, while ratified and adopted by the parliament in 2014.

The main cause for that is obviously due to the series of the well-known political circumstances that Egypt has been through since the break of the so called Arab Spring in January 2011, where Egypt haven't had a stable parliament since 2011 until recently.

Meanwhile, on the 27th of June 2014, the member states of the African union adopted the "African Union Convention on Cyber Security and Personal Data Protection"[33]. The main purpose for this

---

[30] Ibid page55

[31] Ibid28, page 183

[32] Arab Convention on combating Information Technology Crimes http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences accessed 23/8/2016

[33] AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION, Adopted by the 23rd Ordinary Session of the Assembly of the Union, Malabo, 27th June 2014.

convention was similar to that of the Arab convention, however Egypt has not ratified the convention or bring it into force for no known reason until now.

However, ratifying the Arab convention is a huge step on the right direction for Egypt in the field of data protection and cyber security and was, with no doubt, one of the main derives behind the ongoing efforts to adopt the information technology crimes and the cybersecurity law as proposed.

Chapter 2

The proposed law

II- Background

On the 12th of January 2016, the Egyptian ministry of communications and information technology, communicated a bundle of laws to be enrolled in the legislative agenda of the High Committee for Legislative Reform, among which was a law concerning cybersecurity and data protection, "The cybersecurity and Information Crime Law".

The purpose of the proposed law is – apparently – to maintain data protection and privacy of the individuals and the country from the hazards of cybercrime and all sorts of privacy violations.

I will start with a general overview of the proposed law and then see the amount of participation to data protection and cybersecurity the law has and see what could be done for this law to better achieve its goal.

A- Overall structure of the proposed law

The proposed law consists of six chapters.

i- First chapter

The first chapter consists of 4 articles, first article contains definitions that came in a very detailed and long style, consisting of 51 definitions that, in the views of the proposing body, covers all aspects needed for the functioning of the law.

Second article comprised seven points clarifying the main purposes of the proposed law. Third article states the persons, whether natural or legal, who are subjected to the law. While article four about exceptions, mainly from the persons subject to the law, basically national security authorities, taking into consideration the obligation upon such authorities to commit to establish a system in conformity with the minimum standards provided for in the law.

ii- Second chapter

The second chapter is considered to be the most important chapter of the law, as it establishes in 19 articles, from 5 to 23, a new body entitled to monitor the application of the proposed law and was named the "National Authority for Cyber Security", hereinafter NACS.

The articles state the purpose of the NACS, its competence and jurisdiction, the articles also organise how the NACS is formed and the funding thereof.

A further detailed view for the NACS will be dealt with later in this chapter.

iii- Third chapter

This chapter consists of eleven articles, related to the second one and contains the conditions of appointment, and qualifications that the members of the board of NACS should have and ways those members are appointed.

iv- Fourth chapter

This chapter comes in twenty four articles, dealing with the obligations and responsibilities of the persons subject to this law, specifically data controllers, in nine sections. The chapter deals specifically with the responsibility of the persons subject to the law in laying down security policies and drawing the limitations of such policies, dealing with the temporary clearance permits for personnel working for third parties and temporary labour, limitations of the responsibility for managing and administering the information assets, human resources and communication systems, in addition, it regulates the responsibilities of the data controller in taking security measures necessary for access to the network and information and the procedures to be taken when purchasing, renting or maintenance of information systems and the last section puts an obligation on data controllers preventing them to get in contact with any of the persons who are found in breach of the provisions of the law.

v- Fifth chapter

In ten articles, this chapter regulates the work, discipline and appointment of experts.

vi- Sixth chapter

It consists of two sections, first one dealing with interim measures that could be taken and issued by the judiciary, including the measures for seizure of proof and other procedural matters.

Second section states the infringements and the penalties thereof.

The law then comprises three main ideas, the idea of setting a group of definitions encompassing all data related and internet related terms which will be beneficial for the application of the law and can act as a guideline for future laws dealing with the same matter. In addition, it establishes a supervising body, the NACS, which should have a big role in helping this aw in achieving its goals. Lastly, it establishes a set of crimes that are supposed to cover various types of cybercrimes and computer related crimes.

B- Why now?

Security is one of the most important reasons behind the idea of proposing the law at this point, thus in a memo attached to the proposed law explaining the urge to adopt such law at that time, the ministry of communications made it clear that the security concern was one of the most important reasons behind the proposal of the law.

That actually makes sense, as a lot of crimes committed online or using technology in general cannot find an applicable provision in the Egyptian law, thus compromising security on the individual and national level.

For example, if we took denial of service attacks "DOS" and distributed denial of service attacks "DDOS" as an example of cybercrimes[34], Worthy and Fanning argue that the commercial risks associated with DoS attacks are significant. Besides remediation and reputational costs, victims face extra software and consultancy costs together with the risk of increased bandwidth/usage charges (for example, where hosted sites are targeted)[35], however. we will find no competent provision in all of the Egyptian laws dealing with this crime, save for article 361 of the Egyptian Penal code, which does incriminate sabotaging peoples properties, which won't fully apply as long as no tangible harm was done to the devices or computers subject to the attack as the article explicitly applies on "fixed or movable property"[36].

However, security reasons are not the only ones behind the proposal of the law, given the increasing value of electronic commerce in Egypt; thus in an interview for the founder of the famous electronic commerce webpage "Souq.com", Al-Sahi said that the number of people using electronic commerce in Egypt is 9.25 million, expected to reach 15 million by next year, however, he however added that less than 7% of the persons visiting his site actually perform commercial transactions due to the lack of confidence [37], apparently because of the absence of legal platforms protecting consumers data from various sorts of assault.

Both security and economic dimensions of adopting the law at this point are strongly connected, thus, risk management is one of the key issues any donor, especially the IMF which Egypt has been eagerly seeking its loan, until it already succeeded this year[38], might seek, and as cybersecurity will improve trust in the overall security and commercial atmosphere in Egypt, adopting this law at that specific time seems appropriate in strengthening the status of Egypt on the international level.

---

[34] DOS is when a deliberate attempt is made to stop a machine from performing its usual activities by having another computer create large amounts of specious traffic, while DDOS is when one computer controls a large number of remote computers called 'zombies' to organise an attack of a target at the same time. Source: Difference between DOS and DDO <Shttps://hetzner.co.za> accessed 2/1/2016

[35] Bill Gould, Anonymous hackers take down five government websites in whaling protest, http://www.express.co.uk/ accessed 2/1/2016

[36] Art.361 Egyptian Penal Code

[37] E-commerce expanding in Egypt (in Arabic) http://www.aljazeera.net/news/ebusiness/2016/6/5/%D8%A7%D9%84%D8%AA%D8%AC%D8%A7%D8%B1%D8%A9-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9-%D8%AA%D8%AA%D9%88%D8%B3%D8%B9-%D9%81%D9%8A-%D9%85%D8%B5%D8%B1 accessed 10/9/2016

[38] Egypt—IMF talks: Good goals, risky business, http://globalriskinsights.com/2016/08/egypt-imf-talks-good-goals-risk-business/ accessed 19/9/2016

The IMF loan deal with Egypt, recently closed, made a set of conditions in order to affect the loan, a lot of which regarding meeting the conditions set out in the united nations agreement against corruption[39], and as cybersecurity is one of the law on the agreement's checklist, adopting a law for cybersecurity will serve the country's goal in getting the loan at this crucial economic phase.

Chris Jarvis, IMF mission chief for Egypt, said in a statement after the deal was announced, that "Egypt is a strong country with great potential but it has some problems that need to be fixed urgently"[40]

Therefore, securing data will not only enhance security on both national and individual levels, but also will have a positive effect on the Egyptian economy on the long and short terms, promoting trust in the government and enhancing Egypt's image before rating authorities and loan donors.[41]

C- Key articles of the proposed law

It is evident that the proposed law is too vast to be covered here, however, I have chosen some of the key sections that I believe the most are important and could be dealt with in a better way at the final adoption process to provide further details on how the proposed law dealt with it and what enhancements could be introduced to the original draft.

I- National Authority for Cyber Security

As mentioned earlier, the second chapter of the proposed law is dedicated to the establishment of the NACS, the section comes in 19 articles dealing basically with the NACS's aims, jurisdiction and duties, in addition to its structure and sources of funding.

In the latter, I will have an overview of the functioning of the NACS in the proposed law with focus on formation and jurisdiction.

1- Aims of the NACS:

Article 6 of the proposed law stated seven aims for the authority, all stem from its main goal of raising the cyber security capabilities of the country and developing the cyber security industry in the country.

The above mentioned goal comes within the frame of supporting the high interests of the country and its national security; establishing the idea and culture of cyber security in the community; regulating the activities of providing and operating of cyber security services; development of a national industry for cyber security; ensure the compliance with the international treaties effective in Egypt and decisions issued by the international and regional organizations concerning cyber security; monitoring the establishment of cyber security policies and monitoring the enforcement of the law.

---

[39] An interview with Dr. Haitham Albaakli, Counselor at the Egyptian Ministry of Justice, Legislation sector, 18/9/2016.

[40] IMF Steps Deeper Into Middle East Cauldron With Loan to Egypt, http://www.hellenicshippingnews.com/imf-steps-deeper-into-middle-east-cauldron-with-loan-to-egypt/ accessed 19/9/2016

[41] Ibid38

2- Terms of reference of the NACS

Articles 7,8 and 9 of the proposed law deal with the terms of reference of the NACS, among which it has the power to lay down plans and programs and administration techniques suitable to the application of the law, regulate licensing of practice of all cyber security relevant businesses and providing expert consultations to the authorities investigating cyber security breaches.

In addition, article 8 consisted of a long detailed set of powers exclusively for the NACS including technical and administrative rules to be put by the authority to regulate the functioning of the law and coordinating between the different undertakings and putting the main strategy of cyber security all over the country.

Furthermore, the authority is entitled to provide consultations to third parties both on the national and international level after obtaining a written consent from the Egyptian president.

3- Structure of the NACS

Article 14 contains the structure of the authority, it provides that the authority shall be administered by a board of directors of 15 members, to be formed by a presidential decree.

Article 18 provides that the authority should have an executive chief, to be appointed by a ministerial decree of the prime minister for four renewable years, +the executive chief is responsible for the functioning of the authority on the technical and administrative levels, furthermore, the executive chief shall represent the authority before courts.

Article 21 provides that the president of the board of directors shall issue a decision establishing four committees, 1- committee for the regulation of the cyber security professions, 2- committee for the supervision and inspection of cyber security systems, 3- committee for the development of cyber security systems, 4- committee for the development and training of human resources.

II- Criminal and procedural protection

The sixth chapter of the proposed law is considered the core part of the legislation, as it sets out in two sections the procedural protection of data and the crimes and penalties for breaches.

A- Procedural protection

This section consisting of 2 articles deals basically with the collection of electronic evidence and the value of proof thereof.

- **First section**

Article 73 gives the competent judge the authority of issuing instant decisions in the absence of any of the parties to:

1- Seize, withdraw, collect or hold any data or information or any information system and the tracking thereof.
2- Search, entry and access to any computer program, data base, and other devices and electronic systems for the purposes of the execution of the seizure.

3- Order any data controller or information system controller or service provider to hand in any data concerning any information system or electronic system or technical device under his control or saved in his cyber space or on any multimedia, as well as any data concerning communications performed on this system or any technical device.

Article 74 gives the electronic evidence derived from the devices, multimedia, hardware, information system, computer program, or any means of information technology, the same value of proof of physical evidence in criminal proof, on the condition that the procedures approved by the NACS for electronic evidence keeping are followed.

- **Second section**

The second section consists of 10 articles, containing crimes and penalties in addition to the NACS's competence in interfering with initiating legal actions towards any breach and the ability to withdraw any legal actions.

Article 75 and 76 contains a list of crimes – 22 crimes – some of which are purely computer crimes, as the subject of the offence is a computer system or information systems, others are computer related crimes, and those are conventional crimes committed by using a computer or any technological means, in addition to cybercrimes where the internet is a factor in committing the crime.[42]

The overall language of the proposed law seems more technical than legal, the law, mainly drafted by engineers, lacks legal depth, making it very detailed and sometimes redundant.

D- Similar law proposals

On 30/5/2016, the legislative reform committee proposed a law for combating information technology crimes, "The Anti Information Technology Crimes Law".

For the purposes of analysis and comparison, I will mention the basic structure of the law and to deal with it with a slight more details when comparing it with "The cybersecurity and Information Crime Law" later on.

The structure will only focus on the titles of the various chapters and a brief description of articles in order to monitor the apparent similarity between the two proposed laws although the first law is much more comprehensive than the second.

Egyptian law for Information Technology Crimes

First chapter:

General provisions

Art.1 : Definitions

Art.2: rights and obligations of service providers

[42] Computer crime, http://www.lectlaw.com/mjl/cl025.htm accessed 22/9/2016

Art.3: territorial scope of application

Art.4: international cooperation in the field of combating information technology crimes

Second Chapter:

Procedural provisions

Art.5: law enforcement personnel

Art.6: jurisdiction

Art.7: investigation and judicial procedures

Art.8: decisions and orders "concerning granting the right to acquire data or information for the purposes of law enforcement"

Art.9: decisions and procedures concerning requests for blocking websites

Art.10: appealing the decisions issued for blocking a website

Art.11: travel ban

Art.12: experts

Art.13: digital proof

Art.14: reconciliation

Third chapter:

Crimes and punishments

Section 1

Assaults on the integrity of information technology networks and systems

Art.15: illegal use of telecommunication services

Art.16: passing of access "going further the authorized right to login granted by an account owner"

Art.17: illegal access

Art.18: illegal interception

Art.19: assault on the integrity of the information technology systems

Art.20: assault on emails, websites, and private accounts

Art.21: assault on the design of a website

Art.22: assault on information systems of the state

Art.23: assault on the integrity of the information network

Art.24: software, equipment, and tools used in committing information technology crimes

Section 2

Crimes committed using information technologies and systems

Art.25: crimes related to terrorism

Art.26,27: organized crimes committed using information technology systems

Art.28,29, 30,31,32: crimes related to electronic fraud and electronic counterfeiting

Art.33: crimes related to intellectual property violations and related rights

Art.34,35,36,37,38: crimes related to violations of privacy and illegal content

Section 3

Crimes committed by site administrator (admins)

Art.39,40,41,42:

Section 4

Criminal responsibility of service providers

Art.43-47

Section 5

Aggravating circumstances

Art.48

Section 6

Criminal responsibility of legal persons

Art.49,50,51

Section 7

Accessory penalties

Art.52,53,54

Section 8

Attempted crimes and extenuating circumstances

Art.55,56

Fourth chapter

Transitional and final provisions

Art.57,58,59

It is obvious here the criminal nature of this law, it basically enumerates crimes and penalties, unlike the first one that regulates data transmission in addition to stating crimes, however, it deals with more details with cybercrimes committed via the internet.

The reason behind the suggestion of the second law is still not clear, and whether both of them are going to be adopted at the same time or not is something that is still under discussion in the Legislative Reform Committee.

In the next chapter, I will deal with some analysis and critique for some of the main provisions of the law and suggesting enhancements on the original draft.

Chapter 3

Critique of the proposed law

III- Analysis of some of the articles of the proposed law

As mentioned earlier, the proposed cybersecurity and Information Crime Law is too vast to be analyzed in this paper, consequently, I will select three main issues that I find important in the law and see how does the law deal with them.

Those three issues are; the NACS formation, duties and terms of reference, the criminal and procedural protection section, specially, the denial of service attack crime mentioned in the criminal section of law; and the judicial role in search and seizure of information and data.

Dealing with those issues with some details will be followed by recommendations of what I think should be changed and why, and the impact of that change.

A- The National Authority for Cyber Security

It is undisputed that the establishment of the NACS is a huge step and a great accomplishment of the law, thus, establishing an independent authority supervising the application of the law would definitely enhance the functioning thereof.

However, articles that dealt with the regulation of the NACS had some issues regarding what should be put in the law and what should be left for the executive regulations of the law.

The overall wording of the articles dealing with NACS seemed to be extensively detailed for no reason, or at least, most of the details mentioned in the law could be mentioned elsewhere to avoid confusion.

For instance, articles 7 and 8 contain a non-exhaustive list of terms of reference and powers of the NACS that seem very confusing and similar and overlapping in a lot of points, furthermore, some of them are unconstitutional in the first place.

Article 8/4, for example, provides that the NACS is the only authority entitled to suggest relevant laws and regulations, however, constitutionally, the parliament is the legitimate body entitled to legislate and draw the general policy of the country.[43]

Another issue about the articles regulating the NACS formation is that none of the articles of the law dealing with the formation of the NACS provided for the requirements or the competences of the executive chief, although he/she has a very sensitive and powerful position[44] which means that he/she has to have certain qualifications that enable him/her to assume his/her duties.

Lastly, a confusion exists between article 8 providing for the terms of reference of the authority and article 16 stating the powers of the board of directors of the authority, as they overlap in a lot of points confusing what is really meant by each of the articles and whether there is any difference between the two articles or do they complement each other?!

B- Commitments of data controllers

Article 1 of the proposed law defines the data controller as "any person or entity that has the right to establish, store, copy, send, communicate, receive, or extract information or data or the route thereof'. In section four of the proposed law, there is a set of articles regulating the relationship between the NACS and data controllers.

It contains nine subsections that are supposed to cover all aspects of the relationship between NACS and the controllers, however, the articles came in a very detailed way – 27 articles- that contained a lot of provisions making it very complicated for the reader to the law to comprehend and even more, to comply with.

C- Crimes and penalties

Second chapter of section six of the law enumerates crimes and penalties in nine articles. We can categorize the crimes mentioned in this chapter into two main categories.

First one is computer crimes, which is defined as "any illegal act for which knowledge of computer technology is essential for prosecution"[45], and this category consists of two main types of crimes; first are crimes that are computer oriented, which means crimes that are new to the conventional crimes and the subject is usually a computer system such as denial of service attacks and direct data breaches; second type is computer related crimes which are conventional crimes committed

[43] Art.101,122 of the Egyptian Constitution 2014

[44] Art.14 of the proposed law

[45] COMPUTER-RELATED CRIMES, BARRY J. HUREWITZ, ALLEN M. Lo, 30 Am. Crim. L. Rev. 495 1992-1993

by using a computer, and that applies to all sorts of crimes that could be committed using a computer such as certain kinds of forgery and fraud.

Second category are cybercrimes, which are "crimes that are committed via the internet"[46].

The problem about this chapter is that it doesn't categorize the crimes into the above mentioned groups, such drafting style resulted in confusion resulted from the apparent difference in the penalty for a crime committed in a conventional way from the same crime committed electronically, notwithstanding the fact that the articles contained a provision that the penalties provided for are "Without prejudice to any more severe penalty in the Penal Code or any other code".

For example, article 76 makes it a misdemeanor for establishing a website for the purpose of drug dealing, punishable with not less than six months in prison and a fine of not less than 100000LE and not more than 500000LE. However, drug dealing is a felony punishable with death penalty or lifetime imprisonment[47] if committed by conventional means.

Although the articles in this chapter contains a conservatory provision that any punishment set for any of the crimes is "Without prejudice to any more severe penalty in the Penal Code or any other code", such style of drafting often creates confusion in the minds of the readers, especially that according to the Egyptian penal code, if the same deed forms multiple crimes, the crime with a stricter penalty and the judgment inflecting that penalty shall alone be considered[48], which means that the current suggested drafting can be described as redundant when it puts less severe penalties for a conventional crime when committed electronically, because when it comes to the court ruling, the court shall only apply the provision with the more severe penalty.

Another issue concerning the content of one of the most important crimes mentioned in this chapter is what is penalized by article 75 para.12, this paragraph criminalize the denial of service attacks in providing that it's a crime punishable by detainment not less than six month and a fine of not less than 20000LE and no more than 100000LE or either penalties for whoever sends numerous messages in a massive way to an information system or a website of a third party without prior **consent**, or to an unspecified number of persons without their prior **consent**.

The above mentioned provision triggers a problem, that it requires the absence of consent as a condition for the application of the article, however, that caused practical problems before in other jurisdictions where judges used the "authorization" condition to grant acquittal to culprits of DOS. In England, District Judge Grant, sitting as a youth court in DPP v Lennon, where the respondent had been charged under s. 3 (1) of the Computer Misuse Act 1990 ('the 1990 Act') (unauthorized modification of computer material), considering each e-mail sent by the respondent on an

[46] Cybercrime, http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime accessed 26/9/2016

[47] Art.34 law no.182 of the year 1960 for Drugs

[48] Art.32/1 Egyptian Penal code

individual basis, the implied consent to each resulted in implied consent collectively and therefore the modifications made were authorized, dismissed charges against the respondent[49].

D- The judicial competence in search and seizure of data and information

Articles 73 of the proposed law give the chief judge of the competent court, upon request of the public prosecutor, the power to issue interim orders as mentioned earlier in chapter two of this paper to seize and search and collect or withhold data and information in addition to ordering data controllers to hand in any data and information under their control.

This article is one of the most important articles of the proposed law in a lot of ways, first, it strengthens the supervision on the process of collecting data for investigatory reasons by giving it to a judge, thus providing more protection against invasion of privacy by any investigatory body.

The article in its current drafting evades some problems that rise in other jurisdictions as a result of the absence of proper supervision on the process of collecting and processing data.

In the famous European Court of Justice ruling in Digital Rights Ireland[50] , one of the grounds on which the ECJ strike down the Data Retention Directive after Digital Rights Ireland - a human rights advocacy group -, the government of the province of Carinthia and more than 11,000 Austrian residents challenged the legal validity of national laws enacting the directive before the High Court of Ireland and the Constitutional Court of Austria,[51] was that the Directive did not set any limits on the possibility of national authorities accessing the data retained by private companies, and failed to specify conditions that justify the use of these data for law enforcement purposes[52]: "on the contrary, Directive 2006/24 simply referred, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law"[53] and did not make access dependent "on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities [54]".

Similarly, the protection of data from investigatory authorities is protected under the Egyptian constitution in art. 57 as mentioned earlier, and specifically, the article provided that "The right to privacy may not be violated, shall be protected and may not be infringed upon. Postal, telegraphic and electronic correspondences, telephone calls, and other means of communication are inviolable,

---

[49] Andrew Carlesworth, "LEGISLATING AGAINST COMPUTER MISUSE: THE TRIALS AND TRIBULATIONS OF THE UK COMPUTER MISUSE ACT" 1990 4 J.L. & Inf. Sci. 80 1993

[50] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others [2014]

[51] Xavier Tracol, Legislative genesis and judicial death of a directive,The European Court of Justice invalidated the data retention directive (2006/24/EC) thereby creating a sustained period of legal uncertainty about the validity of national laws which enacted it., computer law & security review 3 0 (2 0 1 4) 7 3 6 e7 4 6

[52] Federico Fabbrini, Human Rights in the Digital Age, Harvard Human Rights Journal / Vol. 28

[53] Ibid50 para 60

[54] Ibid50 para62

and their confidentiality is guaranteed. They may not be confiscated, revealed or monitored except by virtue of a reasoned judicial order, for a definite period, and only in the cases defined by Law."[55]

Consequently, hasn't the proposal had such provision, any sort of collection or processing of data for investigatory reasons could have been subject to annulment in court and consequently the annulment of the value of proof of the evidence derived thereof.

In addition, article 74 gave the electronic evidence the same value of proof of the tangible evidence. This article is also important, even if such provision had a similar one regarding granting the value of proof to electronic signatures and electronic documents, same as the value of proof of hand written one[56], however, granting such validity and value of proof to all forms of evidence derived from electronic sources has a valuable effect in giving certainty for the undertakings when dealing with electronic transactions and consequently enhances trust in the cyber world.

IV- Suggestions regarding some of the problematic articles of the law

A- Suggestions regarding the NACS

As mentioned earlier, the articles dealing with the powers and functions of the commissioner, in addition to the articles dealing with the relation between the NACS and the data controllers came in a very detailed and confusing style.

Following the drafting style adopted in the Data Protection Act of England, where the Data Commissioner Office performs a similar task as the Egyptian NACS, it is suggested that articles 35 to 72 of the proposed law dealing with the relation between the NACS and Data Controllers are substituted with an article stating the right of the NACS to issue "Code of Practice" or "Administrative Instructions" to data controllers and relevant undertakings following S.51 of the Data Protection Act of England[57], and penalizing the non-conformity with those instructions and codes.

This will save a lot of confusion and provide much flexibility for the NACS to change its main strategy and regulations for the different undertakings to keep up with the rapid changes in this area.

In addition, omitting article 8/4 of the proposed law giving the NACS the exclusive right to suggest relevant laws and regulations is a must to avoid annulment of such provision for being unconstitutional as explained earlier.

Furthermore, it is suggested that clear and precise criteria for the choice of the executive chief of the NACS is to be mentioned in the law, in addition to a provision declaring the independency of the NACS to insure that the executive authority cannot interfere with its work.

Lastly, most of the extensively detailed articles dealing with the formation and terms of reference of the NACS should be moved to the regulations of the law to avoid confusion and unnecessary

---

[55] Art.57 Egyptian Constitution 2014

[56] Art. 14, 15 of the Egyptian E-signatures law no.15/2004

details in the law, and to be substituted with articles dealing briefly with its terms of reference giving it the right to regulate its own structure and duties.

B- Suggestions for crimes and penalties

Categorizing crimes to cybercrimes and computer crimes and the adhesion to the penalties set for the crimes committed using conventional methods with its electronic counterpart shall remove a lot of the confusion resulting from setting different penalties for the same criminalized act only for using technological methods in committing them.

In addition, to avoid the redundancy resulting from mentioning penalties for conventional crimes committed using technological methods, a provision could be added to the crimes and penalties section provides that "any offence provided for in the penal code or any other law, committed using information technology system shall be punishable with the penalty provided for in the such law".

Furthermore, concerning the DOS offence provided for in the proposed law, the condition of "consent" provided for in article 73/12, shall be omitted to avoid acquittal on the basis of existence of consent, thus, the notion of consent could be confusing and subject to the interpretation of the judge that might– at this stage- lack the necessary knowledge to define consent in a proper way in the field of data protection and adopting a flexible and goal achieving definition.

Lastly, article 84 of the proposed law provides that no criminal actions shall be brought or any procedures thereof regarding crimes provided for in the law unless a written request from the executive chief of the NACS is filed. Furthermore, the executive chef of the NACS has the right to reconciliation in any of these crimes after the approval of the board of directors. This article could be very problematic in a lot of ways.

First, it gives the NACS the exclusive power to initiate criminal actions, and that is a huge authority in the absence of a clear criteria for the appointment of the executive chef entitled to make the decision on whether certain action could be prosecuted or not, opening the door for the abuse of power in certain infringements concerning breaches of privacy from the governmental side.

Secondly, the direct wording of the article suggests that the NACS can hold reconciliation in any of the crimes mentioned in the law, without considering that a lot of those crimes concern individuals that might be harmed directly by the illegal action committed by the culprit, which means that this will bring victims a sense of injustice in the case the NACS held reconciliation in matters that affects those victims without their consent.

Such provision could be subject to annulment for being non constitutional, thus article 57 of the Egyptian constitution provides for the right to the people to privacy, a right that could be compromised if the law gives the NACS the right to hold reconciliation without the consent of the victims of data breaches.

C- The interaction between the proposed Cyber Security and Information Crime law and the Information Technology Crimes law

Obviously, there is a lot of similarities between the two proposed laws, and while the first one deals in more details with data protection on the different levels, the latter's main objective is to provide for crimes and penalties for computer crimes and cybercrimes.

The huge overlap between the two laws makes it unnecessary to adopt both, especially that they are proposed at the same time especially that proposing both of them at the same time has no known reason.

Until this point, no intention to merge both laws into one is evident, on the contrary, it seems that the adoption of the Information Technology Crimes law could come prior to the adoption of the Cybersecurity law[58]. This approach will have its downsides, as one of the key issues for the guaranteeing of the best functioning of the law is the establishment of the NACS, something that does not exist in the Information Technology crimes law.

Furthermore, the proposed Cyber Security and Information Crime law, deals with a much more comprehensive way with data protection in dealing with the different undertakings like data controllers, putting a full policy and strategy for data protection which means more certainty for data subjects, thus making the law more goal achieving.

However, the current existence of CERT Egypt[59], might perform temporarily the same job as NACS, chilling the effect of the absence of a supervising authority for the application of the law and the absence of detailed data protection policy in the Information Technology Crimes law.

D- Towards more international cooperation

As mentioned earlier, Egypt has joined the League of Arab States Convention for Combating Information Technology Crimes in 2014, which is a very good step in strengthening international cooperation in the field of data protection within the Arab world.

However, Egypt being an axial country both in Africa and the world should stretch its efforts to join every possible opportunity for expanding cooperation in the field of data protection. Consequently, joining and ratifying the African Union Convention on Cyber Security and Personal Data Protection seems to be a must for Egypt.

Apparently, joining the African Convention would expand the range of cooperation to cover the African countries as well as the Arab countries covered by the Arab Convention, which means more protection in the field of data protection and cybersecurity.

---

[58] Interview with Councellor/ Baher Zaghloul, department of research in the Legislative Reform Committee of Egypt, 17/9/2016

[59] EG-CERT was established in April 2009 as part of the National Telecom Regulatory Authority (NTRA**).**
EG-CERT is charged with providing computer and information security incident response, support, defense and analysis against cyber attacks and collaboration with government, financial entities and any other critical information infrastructure sectors scoped to Egypt and its mission is to provide an early warning system against malware spreading and massive attacks against the Egyptian critical information infrastructure.
http://www.egcert.eg/about-us accessed 15/9/2016

Furthermore, joining such convention would also strengthen political and economic bonds between Egypt and the signing African countries, such relations shall have a positive effect over Egypt's economy and security.

Conclusion

Egypt is now going through a crucial period of its history, where economic development and security are the main axis of interest in order to reform the country.

Data protection and cybersecurity are main concerns for any developing country, a fact that was acknowledged by the Egyptian government to the extent that it was provided for in the constitution.

The purpose of this paper was to find an answer to the question of whether the proposed law will satisfy the requirements of articles 31 and 57 of the Egyptian constitution or not, and whether the proposed law would help enhancing the Egyptian economy and security.

After going through some of the key provisions of the proposed law and the current situation of data protection in Egypt, a conclusive answer to these questions seems to be hard to reach.

It is of no doubt that adopting such law at this point would have a positive effect in boosting the trust in the economic atmosphere in Egypt, thus, as consumers are increasingly concerned about privacy, loss of trust translates into lost opportunities and revenues for companies.

Recent high profile data breaches have pushed consumers to escape from service providers that did not adequately protect personal data. Consequently, economies offering privacy-friendly services are more appealing to consumers, and this is where data protection laws get their importance in the economic field[60].

As for the security dimension, which was explicitly expressed as the main objective for adopting the law, it is of no doubt that adopting a law that stretches over all sorts of technology related crimes that could not be covered with regular laws would strengthen security both on the individual and national level.

And being the main concern, the proposed law in providing for regulations for data controllers to secure their cyber space and the data contained therein and their information system and network and defining their obligations, in addition to providing for a set of crimes and penalties that covers almost all cybercrimes and computer related crimes[61], the proposed law is strengthening security on both the individual and national level.

Nevertheless, the practical application of the proposed law shall be the real determinant of the success thereof, problems that might arise from the application of the provisions of the law, in addition to the interpretation of such provisions by the judiciary shall be the criteria for the need to significant amendments to the law.

Lastly, adopting data protection laws alone seems to be insufficient for realizing data protection and cybersecurity, international cooperation is a must, therefore, Egypt should make more effort

[60] The EU Data Protection Reform and Big Data, Factsheet, March 2016

[61] Explanatory note for the proposed law on cyber security and information crime, January 2016, annex no.1

in joining relevant conventions and treaties to expand the range of international cooperation between Egypt and other countries, such cooperation shall have a positive effect on the Egyptian cybersecurity.

Bibliography

1- Jonathan Shaw, Why "Big Data" Is a Big Deal, < http://harvardmagazine.com/2014/03/why-big-data-is-a-big-deal>
2- Rick Whiting, 2015 Big Data 100: Business Analytics, < http://www.crn.com/slide-shows/data-center/300076704/2015-big-data-100-business-analytics.htm?itc=refresh> accessed 24/7/2016
3- http://www.guardian.co.uk/world/2012/jan/26/african-twitter-map-continent-connected accessed 15/8/2016
4- http://www.pwc.com accessed 15/8/2016
5- Mohamed N.Elguindy, Faisal Hegazy, Cybercrime legislation in the middle east, information systems security association, Published February 27, 2012
6- http://www.antiphishing.org
7- http://fatwa.islamweb.net/fatwa/index.php?page=showfatwa&Option=FatwaId&Id=45328
8- Quraan
9- , https://www.article19.org/data/files/medialibrary/37966/Egypt-telecoms-report---English.pdf data protection in egypt accessed 30/7/2016
10- Competition law and data www.autoritedelaconcurrence.fr/doc/report**competitionlaw**and**data**final.pdf
11- Comprehensive study on Cybercrime, draft February 2013, United Nations, New York 2013.
12- Patrick Stewart, TRADING CYBERCRIME FOR JOBS AND COMMERCE OR PAYING UP: USING THE WTO TO COMBAT CYBERCRIME, 48 Geo. Wash. Int'l L. Rev. 475 2015-2016
13- Arab Convention on combating Information Technology Crimes
14- AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION, Adopted by the 23rd Ordinary Session of the Assembly of the Union, Malabo, 27th June 2014.
15- https://hetzner.co.za
16- Bill Gould, Anonymous hackers take down five government websites in whaling protest, http://www.express.co.uk/

17- E-commerce expanding in Egypt (in Arabic) http://www.aljazeera.net/news/ebusiness/2016/6/5/%D8%A7%D9%84%D8%AA%D8%AC%D8%A7%D8%B1%D8%A9-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9-%D8%AA%D8%AA%D9%88%D8%B3%D8%B9-%D9%81%D9%8A-%D9%85%D8%B5%D8%B1
18- Egypt—IMF talks: Good goals, risky business, http://globalriskinsights.com/2016/08/egypt-imf-talks-good-goals-risk-business/
19- An interview with Dr. Haitham Albaakli, Counselor at the Egyptian Ministry of Justice, Legislation sector, 18/9/2016
20- IMF Steps Deeper Into Middle East Cauldron With Loan to Egypt, http://www.hellenicshippingnews.com/imf-steps-deeper-into-middle-east-cauldron-with-loan-to-egypt/
21- Computer crime, http://www.lectlaw.com/mjl/cl025.htm accessed 22/9/2016
22- COMPUTER-RELATED CRIMES, BARRY J. HUREWITZ, ALLEN M. Lo, 30 Am. Crim. L. Rev. 495 1992-1993
23- Cybercrime, http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
24- Andrew Carlesworth, "LEGISLATING AGAINST COMPUTER MISUSE: THE TRIALS AND TRIBULATIONS OF THE UK COMPUTER MISUSE ACT" 1990 4 J.L. & Inf. Sci. 80 1993
25- Xavier Tracol, Legislative genesis and judicial death of a directive,The European Court of Justice invalidated the data retention directive (2006/24/EC) thereby creating a sustained period of legal uncertainty about the validity of national laws which enacted it., computer law & security review 3 0 (2 0 1 4) 7 3 6 e7 4 6
26- Federico Fabbrini, Human Rights in the Digital Age, Harvard Human Rights Journal / Vol. 28
27- Interview with Councellor/ Baher Zaghloul, department of research in the Legislative Reform Committee of Egypt, 17/9/2016
28- The EU Data Protection Reform and Big Data, Factsheet, March 2016