BALTIC JOURNAL OF LAW & POLITICS
A Journal of Vytautas Magnus University
VOLUME 15, NUMBER 7 (2022)
ISSN 2029-0454

Cite: *Baltic Journal of Law & Politics* 15:7 (2022): 970-986
DOI: 10.2478/bjlp-2022-007072

Protection of Patient's Personal Data in Telemedicine: A comparative Analysis between the Egyptian and the European Legislations

Akmal Ramadan
1 Professor of Civil Law, City University of Ajman, United Arab Emirates.

Sameh A. Eltohamy
Professor of Civil Law, Zagazig University, Egypt.

Abdul Azeez Yusuf*
Assoc. Professor & Dean, School of Law, Kampala International University, Uganda

Received: October 16, 2022; reviews: 2; accepted: December 23, 2022

Abstract

This study aims to examine the legal aspects of protecting a patient's personal data within telemedicine, by identifying the different trends associated with the concept of personal data, types of data subject to protection and the importance of protecting them. The study also aims to compare the local Egyptian legislation for protecting personal data in Telemedicine with its French counterpart and a few other European Nations. The conditions attached to processing such laws, as enshrined in the Egyptian legislation, and the rights and obligations arising from such a kind of data protection, as well as the civil liability that may result from breaching protected personal data, will also be examined to establish its adequacy or otherwise.

Keywords

Patient, Personal data, Telemedicine, Egyptian legislation, French legislation.

Introduction

The importance of this study lies in the fact that it is one of the contemporary legal discourses originating from the development accomplished through the modern means of information communication technology systems. The

importance of selecting a subject matter relating to personal data protection for a patient being medically monitored remotely lies in the economic and moral values that are attached to it. Therefore, there is a need to develop an appropriate legal system to protect these values. In addition to that, the emergence of various forms, patterns, and images of data abuse on the internet in different sectors, especially in the medical field and workplace call for jurisprudence and judicial review to address this phenomenon through the formulation of a daunting legislative system that will not only protect the patient's personal data but also will remotely hold any culprit liable for any abuse. In view of this, the study shall first examine the concept of a patient's personal data placed on remote medical monitoring and the importance of protecting it. Secondly, the study will take a critical look at the legal means of confronting an attack on a patient's personal data on remote medical monitoring. Thirdly, the conditions attached to the processing of the laws governing a patient's personal data in Egyptian law will be examined in comparison with few other European legislations.

Importance of protecting patients' data in telemedicine

Patients' data is important not only to its owners, but also to their families and community as it is part of the personal data that is worthy of protection. How can one imagine a life without the protection of personal data? Can one be at ease in the world of internet and electronic transactions, financial, banking or other services? Could there be any trust in social networking sites such as Facebook, Twitter, WhatsApp, Instagram, Snapchat, etc.? Is there any guarantee for the protection of one's data in different institutions and sectors like health, employment, education and other sectors, such as the military and finance, which house data that are of national interest? It is because lack of adequate provisions that guarantee the protection of the privacy of these sensitive personal data that makes it imperative for some of these institutions to employ their capabilities and strategies to put in place some mitigation plans that will constantly protect their data and ensure that they are neither encroached nor attacked. Given that, the above-raised questions made us realize the importance of the need to protect patient's data, especially in the contemporary era of "big data" resulting from the steady use of digital devices, computers, and every other thing that is connected to the internet, especially in the present era of digitalization and interconnectivity of apparatus, devices, homes and other technical facilities to the internet, The personal data of the user is no longer limited to name, photo and phone number, as was the case at the beginning of the internet, that, which in recent time, had expanded to include vital data for users, such as eye, face, hand and fingerprints and many other personal data related to the quality of foods, drinks, clothes, movies, books, and music in different sectors like health, finance, and other geographical location and path of movement, as may be desired.[1]

[1] See Al-Ittihad Newspaper: dated 27/6/2018; https://www.alittihad.ae/wejhatarticle/99484/%D8 Accessed on 27/4/2020.

If one takes a look at the large number of companies and industries around the world, one would see that they have a massive amount of data in their records, such as that of shareholders, investors, employees, customers, product information, financial transactions, and others, and these data are one of the most important assets owned by these companies. They are, therefore, required to protect these data electronically and manually through the provision of a sound risk mitigation plan and enacting internal policies and regulations that will ensure its adequate protection, as bad things could happen when data that needs to be kept in private falls in the wrong hands. A data breach at a government agency can, for example, put highly classified information into the hands of an enemy or hostile country. A company's information breach can put proprietary data in the hands of a competitor, and a breach in school information can put students' personally identifiable information in the hands of criminals who may use it to commit identity theft. A hack in a hospital or doctor's office or workplace can put protected health information in the hands of those who might misuse it.[2] Every invention or discovery, no matter how developed or protected it may be, is vulnerable to certain incursion that makes it possible for an unauthorized person to access other people's data, especially on internet and social networking sites.[3]

Ensuring the protection of patients' data in telemedicine is the slightest thing that patients expect from the remote medical provider because it assures them that their reputation will not only be protected but that such action establishes that remote medical provider as a brand that people could trust when it comes to data protection since a data breach could destroy the trust that might have been built up over the months or years.[4] : The adoption of personal data protection for those on remote medical care was further enhanced due to the growth and widespread linkages of medical stuffs and apparatus to internet, a system which allows the medical experts to record their daily works and health facilities remotely. All these, in the long run, constitute big data which spelt out the relationship that exists between the patients and the providers of the health care services, in terms of the type of disease, psychological state, results of tests, radiology, medicines that are used or recommended and other health data. That is why, in 2019, the Information Commission Office (ICO) of the United Kingdom[5] imposed a fine on a London-based drugstore, Doorstep Dispensary Ltd., for failing to provide medicines to customers and care homes after taking their data. A fine of £275,000 was also imposed on the drugstore for failing to protect customers' personal data by leaving nearly five hundred thousand (500,000) documents in unlocked containers at the back of its headquarters in Edgware, England. The documents stocked inside the containers consist of the names, addresses, dates of birth, National Health Service (NHS)

[2] Clare Stouffer, What is Data Privacy and why is it Important. 19 January, 2021, https://www.lifelock.com/learn-identity-theft-resources-what-is-data-privacy-and-why-is-it-important.html. Accessed on 20/9/2020.
[3] Dunya al-Karjati, Amn al-Bayanat wa al-Ma'lumat. 13/1/2019. https://www.mlzamty.com/search-information-data-security/ . Accessed on 25/4/2020.
[4] Leo Besemer, why is Data Protection so Important? 11th July, 2018. https://www.exin.com/data-protection/why-is-data-protection-so-important/. Accessed on 25/4/2020.
[5] It is a UK independent body established to support the right of information in the interest of the public, and to promote openness among the public institutions and preserve the privacy of data of individuals.

numbers, medical information, and prescriptions for an unknown number of people. Those fines were imposed because the data were not processed in a manner that ensures adequate security against unauthorized incursion or illegal processing, which constitutes a violation of the General Data Protection Regulation.[6] Similarly, Bayswater Medical Center, London, 2018 was fined £35,000 by the ICO after leaving highly sensitive medical information in an empty building for more than eighteen (18) months.[7] The attack on personal data occurs constantly, but very little is disclosed or exposed to the public due to some reasons, such as if the companies or websites do not have sufficient mitigating security plans capable of detecting an attack, or because of fear for their reputation or lack of confidence in their ability, or due to material loss that could be incurred as a result of fine that may be imposed by the law enforcement agencies or due to compensation that may be awarded in favor of those that are affected. [8]

Concerning the Egyptian legal system, the judiciary has pointed out the importance of personal data and considered it as a private matter of an individual. Hence, it is not permissible to break into it, snoop on it, or misuse some aspects of it. The decision of the Supreme Constitutional Court on the matter clarifies that: "there are certain areas of the private life of an individual, such as personal data which is not to be accessed by an authorized individual, and therefore, it is not legitimate for anyone to break into it because it is a confidential matter that is protected and preserved. Therefore, any attempt to eavesdrop on it or snoop on it, either through the modern scientific development that has a far-reaching impact on the daily lives of the people or through any means of technological advancement which has reached an astonishing level in this modern era, should be ward off because leaving it free for anyone to access those private matters and without it being protected may cause embarrassment or harm to their owners. What is understood from that position is that the characteristics of protection of private data and its preservation from intrusion safeguard two interests and features that may seem to be separate but which in reality, are complementary, as they relate in general to the scope of individual's independence and the right to private life that ought to be preserved and protected by law, even though some constitutional documents do not categorically stipulate this right in texts, but it is explicit on it, and that is the more reason why some of the jurists consider the right to private life as one of the most comprehensive and expansive rights that is deeply connected to the values being called for by the civilized nations.[9] The importance of having a personal data law signifies an economic prominence for such a country, as it increases the country's reputation and confidence of customers and investors in the institutions and companies operating in that country. The personal data law will also ease the transfer of data from one country to another, especially when

[6] For details, see the website of Information Commission Office at https://ico.org.uk/about-the-ico/news-and-events. Accessed on 25/4/2020.
[7] See Ibid; https://ico.org.uk/action-weve-taken/enforcement// as accessed on 25/4/2020.
[8] Toby Mendel, Andrew Puddephatt, Ben Wagner, Dixie Hawtin, Natalia Torres, Global Survey on Internet Privacy and Freedom of Expression, UNESCO, 2012, p. 51.
[9] The Supreme Constitutional Court of Egypt. Constitutional Case No. 207, dated 1/12/2018. P. 39 at www.eastlaws.com.

some countries prohibit the transfer of data to a country that does not provide the same level of regulations for personal data protection.[10] The absence of law criminalizing attack or intrusion on personal data may lead to the commission of many crimes. For example, a data breach in a government agency may lead to placing highly confidential information in the hands of an opponent country.[11] Therefore, any penetration by that unfriendly country into any company that is operating in the other country could lead to leakages of data to an opposing country. According to some jurisprudence, the acknowledgment of protection of personal data is an acknowledgment of a person's right to preserve his privacy. It also means an acknowledgment of the right of the state to view and process this data within a specific and clear legal and regulatory frameworks that allow the competent authorities to prevent the occurrence of acts that may breach security and order or to prosecute and punish the offenders. The European Union, on the other hand, is able to put in place very strict measures regarding the transfer of personal data to and from any of its member states.[12] is requirement is applicable in any of its dealings when exchanging personal data with any country outside the European Union territory, especially if such a country cannot provide a level of protection similar to those in operation within the European Union territory.[13] It is, therefore, in the interest of the countries that deal with the European Union to rise to the level of such a protection that the European Union provides, or at least try to be compatible with the ones provided within the European Union so as to affirm their non-exclusion when it comes to dealing with them, because the issue of transfer of personal data from one country to another as well as its protection is more or less the same as the exchange of economic and information communication technology.

Personal data protection under the Egyptian Laws

Regarding the personal data protection law in Egypt, Law No. 151 of 2020, titled: the Egyptian Personal Data Protection Law, was issued after two years of deliberation in the Parliament. This was as step towards the beginning of formation of legislation to protect the personal data of citizens as there was no any existing law on personal data protection in Egypt before then. Analytically, the Egyptian Personal Data Protection Law contains fourteen articles. The first article contains the definition of terms like personal data, sensitive data, data processing, owner, holder, administrator, controller, the processor of data, and other terms. The article also stressed that the provisions of the law and the accompanying law regarding the protection of personal data, with respect to natural persons, are to be processed

[10] Ahmad Saeed, Dirasah Qadhaiyyah. Al-Bayan Newspaper, U.A.E, dated 15/6/2019, at https://www.albayan.ae/across-the-uae/news-and-reports/2019-07-25-1.3613428. Accessed on 17/4/2020.
[11] Muna al-Ashqar Jabur and Mahmud Jabur, Al-Bayanat Al-Shakhsiyyah wa al-Qawanin al-Arabiyyah, Al-Hamm al-Amni wa Huquq al-Afrad: Abhath wa Dirasat. Al-Markaz al-Arabi li al-Buhuth al-Qanuniyyah wa al-Qadhai yyah. Majlis wuzarai al-Adl al-Arab. Jamiat Duwal al-Arabiyyah, Beirut, 2018, p.22.
[12] Clare Stouffer, Ibid., https://www.lifelock.com/learn-identity-theft-resources-what-is-data-privacy-and-why-is-it-important.html. Accessed on 19/4/2020.
[13] See Al-Laihat al-Ammah al-Orobiyyah li himayat al-Bayanat al-Shakhsiyyah, no. 679, Chapter 5, section 44-50, 2016.

electronically in part or in whole by the holder of the data or by an officer. [14] The second article of the law stipulates the rights of the owner of the data and the conditions for collecting and processing of the data. It emphasized that personal data may not be collected, processed, disclosed or revealed except with the owner's express consent or as may be authorized by the law. Other rights mentioned in that same article are the right of cognizance to personal data held by the holder, controller, or processor. Others are his right to view, access, or obtain it, the right to withdraw the prior consent to keep or process it, the right to correct, modify, erase, add or update, and the right to limit the processing of the data within a specific scope, the right to be mindful and aware of any breach or violation of the data, and the right of objection to the processing of the data. It also stipulates the conditions attached to data collection, processing, and retention, such that it must be for a legitimate purpose, precise, accurate, and secured, and it must not be kept longer than the period necessary for it to be renewed. The article further states that the provisions of this law are applicable to all those who commit any of the crimes stipulated in the accompanying law, as long as the offender is an Egyptian residing inside or outside the Country or when the offender is a non-Egyptian residing inside the Republic, or when the offender is a non-Egyptian residing outside the Country, so long as the offense is stipulated to be punishable in the country in which it occurred, and as long as the data related to the crime is for Egyptians or foreigners residing within the Country.[15]

The third Article listed the obligations of the controller and processor of the data, among which is that it is essential to obtain the consent of the owner of the data, verify the authenticity of the data, and set the methods and standards for processing the data in accordance with the purpose that is meant for. It adds that the controller or the holder or the processor of the data should refrain from any action that may lead to the leakage of the data and must take all technical and organizational measures to protect, secure and preserve the confidentiality of the data, so that it would not be breached, altered or tampered with. It is also stated in the article that the data should be erased immediately at the end of the purpose by which it is listed or meant for. It is also compulsory for the person in charge of the data to correct any error found in it as soon as he is informed about it or learnt about it. A remarkable record of the data must be maintained, and a license or permit from the authority must be secured before dealing with the data.[16] In addition, the article stressed that the controller or the processor must notify the authority within seventy-two (72) hours of damage or breach of personal data. However, if the breach or damage is as a result of protecting national security, the report must be lodged immediately.[17] The article further stipulates the data to which the law's provisions could not be applied. These are personal data of natural persons that are not concealed from people to access or be processed for personal

[14] Egyptian Personal Data Protection Law 151 of 2020, section 1.
[15] Ibid., section 2.
[16] Ibid., section 4.
[17] Ibid., section 7.

use only or the data that is acquired for obtaining official statistical data or for the application of legal text.[18] The article further adds that the economic law courts are to look into the crimes specifically mentioned in the provisions meant for it.[19]

The fourth article deals with a data protection officer's appointment and duties. In contrast, article nine of the law stipulates the need for establishing an economic generated public authority to be known as "Personal Data Protection Center" with artificial legal status and with the aim to protect, process and dispose of personal data. It is also established to set up plans, implement decisions, and control and set data protection standards. The Centre is also responsible for establishing memoranda and conclusion of agreements, issuing annual reports on the status of the protected data, offering opinion and advice, and carrying out inspections.[20] The different kinds of licenses, permits, accreditations, and conditions for issuing, obtaining, revoking as well as the prescribed administrative penalties, are the items spelt out in article nine,[21] while it stipulates in article eleven that the center shall have a special budget which shall be prepared in the pattern of economic budget.[22] Article twelve, on the other hand, provides for modes of appeals and complaints,and article thirteen stresses that the center's employees have the capacity of judicial police in crimes that violate this Law's provisions.[23] Finally, article fourteen states the types of crimes and penalties existing under this law when it specifies that "without prejudice to any other severe penalty stipulated in any other law, and without prejudice to the right of the injured to compensation, anyone who violates the provisions of this law shall be punished with imprisonment and a fine or one of the two penalties. The period of imprisonment and fine may vary according to the nature of the offence. The minimum fine as the law prescribes fifty thousand Egyptian pounds, while the maximum is five million Egyptian pounds.[24] However, an accused in any of the criminal case may reconcile with the victim or with the private agent of the victim or with the principal successor of the victim, provided that this is done before the final judgment is issued, and with the approval of the Personal Data Protection authority in front of the Public Prosecutor or the competent (economic) court, and in accordance with the conditions stipulated in the law.[25]

An accused, who wishes to reconcile, is obliged by the law to pay certain amount of money that is equivalent to the half of the minimum fine prescribed on the crime, provided that he either pays up the remaining balance after filing the case and before the issuing of the final judgment, or pay the value of the fine as decided or pay whichever one is greater among the two, and on the condition that the payment be made into the treasury of the court or to the Public Prosecution bureau or to the Personal Data Protection Authority. Thus, with this kind of

[18] Ibid., section 3.
[19] Ibid., section 5.
[20] Ibid., section 19.
[21] Ibid., section 26-30.
[22] Ibid., section 31.
[23] Ibid, section 34.
[24] See Ibid., sections 35-48.
[25] See Ibid., section 49.

reconciliation, the criminal case comes to an end provided that the rights of the victim will not be affected or truncated.

A proper examination of the Egyptian Personal Data Protection Law shows that the Egyptian legislator borrowed some legislative ideas from the European Union General Data Protection Regulation (GDPR). However, some jurists believe that Egyptian legislator is able to make some amendments to some of these rules, especially the ones that concern the rights of an individual whose personal data is to be shared with different parties, and it also guarantees the protection of the right to privacy for the owners of the data. The other additional development noted in the law is that it can align the procedures for activating the data protection law to the executive rules. Though the law is yet to be released, it is an important legislative step that may take a lot of effort to implement.[26]

Despite the novelty of the law, the Egyptian legislator is criticized for exempting some entities and institutions from being subjected or answerable to the provisions of the law. Those exempted, for example are institutions like the Central Bank and national security agencies. The researcher is, however, of the opinion that the Egyptian legislator should have excluded certain types of data that these institutionthese institutions may possess may possess in the course of carrying out their duties from being subjected to the law instead of exempting all personal data and information held by these institutions from being subjected to the provisions of the law, or by restricting the owner of the data from enjoying certain rights when the processing is related to national security or the central bank, because there is probability that leaving these institutions without any restriction could leads to violation of the principle of the rule of law. Therefore, these entities must be subjected to the same regulations that guarantee the protection of the privacy of individuals, more so when the banking sector is supposed to be subjected to greater protection by virtue of the nature and sensitivity of financial data which required more than normal protection. Another defect that is found in the law is that it only provides for the protection of personal data that is electronically processed. However, digital and electronic transformation has not reached its peak in the governmental or non-governmental sectors in Egypt as most personal data are still being processed by traditional non-electronic methods and without guiding laws. Therefore, the law must be applied to both the electronic and non-electronic processed data.[27] Thus, the researcher is of the view that it should be expressly mentioned in the law that the provisions of the law shall apply to all other institutions or individuals that carry out any processing on individual personal data, be it electronic - in whole or in part -, or non-electronic.

In a nutshell, the Egyptian legislator, by making this law, has adopted the global approach in protection of personal data, as we have discovered that the source of the law is the European Union General Data Protection Regulation

[26]Qanun Himayat al-Bayanat al-Shakhsiyyah: Ta'aziz li al-Haqqi fi al-Khususiyyah am Iham bi tahsin al-Biat al-Tashri'iyyah. Published in the website of Masaar Mujtama'in al-Taqniyah wa al-Qanun on 5/12/2020. https://masaar.net/ar/%D9%82%D8%A7%D9%86%D9%88%D9%86-%. Accessed on 9/10/2021.
[27] Ibid., Accessed on 26/3/2022.

(GDPR), and most countries have also adopted similar regulation because it is an all-inclusive personal data protection regulatory framework.[28]

Personal Data Protection in other comparative legislations

Some foreign countries and united states have taken the lead in the proclamation of personal data protection law. Among the proclaimed laws are the Council of European Convention 108 on Data Protection, European Directive No. 46 of 1995 on processing personal data, and General Data Protection Regulation (GDPR) No. 679 of 2016. An attempt will now be made to give an account of each of these regulations as detailed below:

The Council of Europe Convention for the Protection of Individuals with regard to automatic processing of personal data (No. 108 of 1985)

Convention 108[29] is regarded as the basis from which the right to data protection sprung up in Europe, which is why Europeans celebrate Data Protection Day on January 28 annually. It was and remained the first legally binding international instrument in the data protection field. The principles laid down in the Convention are to be applied by the parties to ensure respect in their territory for the fundamental rights of all individuals with regard to processing of personal data by both the private and public sectors, including the data processing that judicial and law enforcement authorities may carry out. The Convention, in addition to that, seeks to protect the rights of individuals and regulate the flow of personal data across the borders.[30] It also aims to provide a safety atmosphere regarding the collection and processing of personal data, and prohibit the processing of "sensitive" data based on race, politics, health, religion, sexual life and criminal record.[31] The convention also protects the right of individual to know whether his data is being stored, modified, or erased.[32] The rights under the Convention can only be restricted when overriding interests, like security of the state or defense and so on are at stake.[33] It also imposes some restrictions on the cross-border flow of personal data and information to countries where their legal regulations do not provide for similar protection.[34]

European Directive 1995/46 on the processing of personal data

Prior to the issuance of this directive, personal data protection was not an

[28] Ibid.
[29] The Convention was opened for signature on 28 January, 1981, and was put into operation on 1st January, 1985. The Convention 108 was modernized in 2018 and was renamed Convention 108+ so as to create a common legal space for the European Union General Data Protection Regulation. For details, see https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000016807c65bf. Accessed on 22/7/2020.
[30] Lydia F de la Torre, what is "Convention 108"? Jun 26, 2019, Posted in the following link: https://medium.com/golden-data/what-is-coe-108-3708915e9846. Accessed on 22/7/2020.
[31] See Article 6 of Council of Europe Convention 108.
[32] See Ibid., Article 9.
[33] See Ibid., Article 11.
[34] See Ibid., Article 14.

entirely new issue in Europe because there is already a legislative framework regarding processing personal data. Directive 46[35] of October 24, 1995 is the main European Union (EU) law on data protection and it is the common basis for all EU countries in terms of personal data protection as drafted and approved at the Council of European Convention 108.[36] The directive defines what personal data is and sets principles for the identification of quality data, the legal basis for its processing, types of authorized bodies or institutions, right of individuals to access their data,[37] consent to handing over data, right of objection, privacy and security of processing, and right to be notified when processing. Article 29 of the Directive also allowed for the establishment of a group that brings together the representatives of national data protection authorities of the parties to the Convention every two months and was nicknamed "G29",[38] with the particular aim to adopt the recommendations that relates to protection of personal data for the European Commission.[39] Although, the directive gives room for harmonization of laws. However, the laws are fragmented among the Member States regarding the protection of individual personal data. French and English legislations, for example, differ on some issues, such as the definition of personal data and the conditions for transferring and processing personal data. This divergence is emphasized in the 2016 regulation, which explains that: there is still that "legal uncertainty or widespread general feeling that a significant risk exists when it comes to the protection of individual personal data, especially if it relates to data that flows between the countries through the internet". Therefore, the provisions of this Directive have shown that it is not adequate enough to cope with the modern technological advancements and the remarkable developments in the digital universe that greatly facilitate the flow of this data. It, therefore, became necessary to intensify individual protection while simplifying the administrative procedures for companies or establishments that use this personal data and preserving the free movement of this data. Consequently, the draft to amend this directive was submitted on 25th January 2012 by both the European Parliament and the Council.[40]

General Data Protection Regulation (GDPR) 2016/679

After 20 months of discussions and 250 hours of informal negotiations between the member states, the European Members of Parliament voted in favor of a data protection package consisting of regulation and a directive in April 2016 and put into effect in May 2018. The regulations is meant to protect the processing

[35] For details on this Directive, see https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A31995L0046 . Accessed on 22/7/2020.
[36] Emmanuel D. Jouffin, Présentation du Règlement général sur la protection des données, Hors-série Banque & Droit – mars-avril 2017, p2.
[37] See Barthélémy Gaillard, Données personnelles: que prévoit l'Union européenne? 16/12/2020, Posted in the following link: https://www.touteleurope.eu/actualite/donnees-personnelles-que-prevoit-l-union-europeenne.html. Accessed on 22/7/2020.
[38] In France, the National Data Authority is known as the National Committee for Data and Rights.
[39] See Jean-Philippe Sala-Martin, 2012, https://www.journaldunet.com/ebusiness/le-net/1029637-donnees-personnelles-vers-une-responsabilite-accrue/. Accessed on 22/7/2020.
[40] Ibid., Barthélémy Gaillard, Accessed on 22/7/2020.

of personal data and it adapts the 1995 directives to the changes in the digital environment, as explained by Carol Ulmer, the Director of Studies at the European Center for Conflict Studies that: "The spirit of the text is clear. It is all about offering a common vision for the protection of personal data in Europe and strengthening the rights of individuals over their data.[41] Therefore, it is inferred from that statement that the regulation is nothing but an EU broaden legal framework for protecting the rights of its citizens, their personal data and information from unauthorized processing. Thus, the General Data Protection Regulation, currently, takes charge of protecting and preserving all the principles upon which the Union's personal data protection system is based. The Regulation also confirms that protection of data is to be transmitted across the borders alongside with the personal data at the same time.[42] The regulation, in addition to that, contains other rights like the right to delete or repeal a data." For example, if a person asks a company to erase certain data, the company must act on it by forwarding such a request to any party that can process such data. Others are right to modify, the right to decline, the right to restrict data processing, the right to transmission or movement of data, and the right to access to data.[43] It also contains various other measures that allow every individual to be informed about the use of their personal data, and it introduce policy changes on how to deal with data that are inscribed in tiny manner. It then adds that the data must be transmitted in "simple and clear" language so that the individual owner can give clear and explicit consent to the processing of his or her data.[44] It also states that the forensic laboratories must notify the users or customers in the event of data breach.[45] Finally, it is emphasized that the aim of the regulation is to encourage the offices and agencies to own and implement good data management system and methods that respect the principle of data protection for their products. In the event of an infringement, the regulations state that any person who has sustained material or non-material damage due to violation of these regulations is entitled to compensation from the controller or the officer in charge of processing the damage incurred.[46] It also provides a fine of up to 4% of the company's turnover worldwide.[47]

French Role in protecting individual personal data

French legislator is considered as one of the forerunners and pioneers of laws in the field of personal data protection[48] through the issuance of Law 17-78 of 6th January, 1978 relating to the processing of data and files, including other amendments that follow, such as amendment 801 of 2004 concerning the

[41] Ibid.
[42] See the official website of Czechoslovakian Regulation for protection of personal data, https://www.uoou.cz/gdpr-obecne-narizeni/ds-3938/p1=3938. Accessed on 23/7/2020.
[43] See the European General Data Protection Regulation (GDPR) 2016/679, Articles 15-23.
[44] See Ibid., Articles 12-14.
[45] See Ibid., Article 33.
[46] See Ibid., Article 82.
[47] See Ibid., Article 83.
[48] Sweden, in 1973, is the first country among the European nations to issue the laws on individual personal data protection, and followed in 1978 by Germany, France, Denmark, Norway and Austria, and Luxembourg later on in 1979.

protection of individuals concerning the processing of personal data that came in line with the European Directive No. 46 of 1995 with regard to the protection of natural persons in relation to the processing and transmission of personal data, as was subsequently amended in 2019 by Law 2019/536 in line with General Data Protection Regulation (GDRP) 2016/679.[49] A critical look at that French Law 2019/536 shows that it contains five sections with regard to individual personal data protection. For example, the second section regulates the regime of protection and processing of personal data in line with what is stipulated in the EU Regulation 2016/679, such as the rights related to the data and the obligations of the controller or the processor of the data. The third chapter regulates the laws that apply to the processing of data under the EU Directive 2016/680 of the European Parliament and Council on the protection of individuals in terms of processing of personal data by competent authorities for prevention and detection of criminal offenses, investigations, and prosecutions, implementation of penalties, free movement, and erasure of data in accordance with the EU Council Convention 2008/977. Section four of the law contains the law that applies to the prevention of threats to public security, state security and defense, while the fifth chapter contains the provisions that relate to other territories.[50] In addition to these regulations, it is stipulated in Article 9 of the French Civil Code that "everyone has the right to respect of private life". In contrast, the French Penal Code, on the other hand, stipulates that a person shall be liable to the punishment of imprisonment for a period of one year and a fine of forty five thousand (45,000) euros for voluntarily infringing the privacy of others by:

1. Capturing or recording or transmitting the words uttered in secret or in private without the owner's consent.
2. Fixing, recording or transmitting the image of a person in a secret place without the latter's consent[51].

European Personal Data Protection Regulation and Health related data

The European, Personal Data Protection Regulation, defines health-related data as: "personal data relating to physical or mental health of a natural person, such as the health-care services which discloses information about the state of health of an individual",[52] while it defines "inherited" genetic data as: "personal data related to an inherited or acquired genetic characteristics of a natural person which provides unique information about the physiological aspect or health of that natural person as a result of the person's specific biological characteristics."[53]. As for the Egyptian law, it mentioned genetic data when defining what is meant by sensitive data without referring to the meaning of genetic data. We, therefore, believe, that the meaning of

[49] For details, see https://www.cnil.fr/fr/la-loi-informatique-et-libertes. Accessed 21/7/2020.
[50] These are the Islands under the French protectorate.
[51] See sections 1-226 of the French Penal Code as contained in the amendment of 5th July, 2020.
[52] See the European General Data Protection Regulation (GDPR) 2016/679 Op.Cit., Articles 4-15.
[53] Ibid. Articles 4-13.

this type of data in Egyptian context should not be different from the way it was specifically defined in the European regulation. It is pertinent here to note that these data explicitly belong to the patient, whether they are those that are related to the type and nature of the disease, results of tests, x-rays, types of medications being taken, as well as other health and psychological data. Other information contained in the health data are those related to the treatment and drug prescribed by the physician in terms of the name of the drug, dosage, drug identification number, price of the drug and the reasons for using it. Therefore, disclosure of a person's medical or health data may result in serious consequences and damages that could affect an individual's psychological state and reputation in the community, given the fact that protection of privacy health and medical treatment is an ethical and legal rule that a physician must not violate, for being an important and professional obligations that must be respected and protected by a physician in honor of the privacy entrusted to him by his patients.[54] This is an ethical and legal duty as required by the principles of honor, honesty and trust due to coming in close contact with an individual's private life. These laws and the various penalties attached to it are, therefore, necessary to maintain the privacy of the personal data of an individual patient in order to ward off or limit the attack on it. Accordingly, an individual's health status is considered a personal right which has to be guaranteed by legal texts to protect the medical privacy of the patient and preserve the confidential professional identity of the health service provider[55]. It was not surprising when it is discovered that Article 5 of Law 2016/4 with regard to medical liability affirmed that: "a physician is prohibited from revealing a patient's confidential issues which he came to know at the course of practicing his profession, regardless of whether it was disclosed to him by the patient or seen by the physician himself or was disclosed to him on trust." Also, Article 4 of Law 2019/2 with regard to the use of information and communication technology in the health fields stipulates that it is mandatory to maintain the confidentiality of health data and information by not allowing it to be circulated or transmitted, except in authorized cases. Some judiciaries in some countries have also established the fact that an individual's personal health and diseases that come with it fall within the scope of private life. Therefore, both of them are regarded as parts of medical privacy, so it is not permissible to publish anything related to an individual's health data except after permission to it has been obtained from the competent authority.[56]

Recommendations on areas to be improved upon by the Egyptian Legislator

After we had examined the Egyptian law and the European legislation on

[54] The law regarding medical liability was issued in the Federal Law No. 10 of 2008 and Administrative Resolution No. 30 of 2017 which approved the regulation for online and remote health services. Article 9/4 further states that the professional physician must be committed to protect the privacy of the patient, preserve the patient's confidential health issues that he has access to during the course of carrying out his professional duties, and he should not divulge those confidential matters except in accordance with the legislation that is applicable in the country.
[55] Ibn Haydah Muhammad, al-Haqq fi al-Khususiyyah fi al-Tashri' al-Jazaairi: Dirasah Muqarana, M.A Thesis, Universite Ahmed Draia d'Adrar, 2010, p.66.
[56] See Ibid., p. 63.

personal data protection, we discovered that the following areas which we are proposing as recommendations needed to be improved upon by the Egyptian legislator so as to strengthen, boost and enrich the Egyptian Laws on data protection in general and the patient's medical data and privacy in particular:

1. It is recommended that the text of Article (3) of the Egyptian personal data protection law 2020/151 should be amended by deleting the fifth and sixth paragraphs which stipulate that all the data related to the National Security and the central bank should be exempted from being subjected to the law. It is, therefore, our opinion, that what the Egyptian legislator should have done is to exclude certain types of data that these institutions may possess from being subjected to the law instead of exempting all the personal data and information held by these institutions from being subjected to the provisions of the law, or by restricting the owner of the data from enjoying certain rights when the processing is related to national security or the central bank, because there is probability that leaving these institutions without any restriction could leads to a violation of the principle of the rule of law.

2. The narrowness of the application of the law by the Egyptian legislator to electronic processing only contrasts with other similar laws existing in the European Union nations. It is therefore suggested that the law be expanded to include any kind of processing, be it electronic or manual or other means of processing.

3. We suggest that Article one (1) of the Egyptian personal data protection Law should be amended by adding the words: "non-electronic processing" so that the text of that article would now read as follows: "the provisions of this law and the accompanying law with regard to protection of personal data must be processed electronically or "non-electronic" - partially or completely - by any holder or controller or processor, especially when the data is related to natural persons. We also suggest that for definition of processing to be an all-compassing, it should include "manual processing" too.

4. The Egyptian legislator stipulates how a data could be processed without indicating that those means as highlighted in the law are just for example, and that there are other technical means of data processing and operation, such as writing, collecting, recording, storing, preserving, merging, displaying, transmitting or receiving, all of which are not contained in the law. Therefore, in view of that, we suggest that the Egyptian legislator should indicate that the operations, as indicated in the law are just for example, and that the law accommodates any other means of processing and operations of personal data even if it is not mentioned therein.

5. The Egyptian legislator did not define the term: "approval". Therefore, we suggest that it is imperative upon the Egyptian legislator to define what is meant by "approval" of the owner of the data in the article on definitions, and to stipulate the criteria and conditions attached to this kind of approval.

6. The Egyptian legislator did not specify the legal age, which requires

the consent of the guardian, the same way it is clearly indicated in the European regulation, and therefore, we suggest that the legal age should be stipulated to avert any dispute or argument.

7. The Egyptian legislator did not specify the cases in which the right to erasure of data could be applied, the same way the European legislator stipulates it in the European Union Regulation for Protection of Personal Data. We, therefore, suggest that provision should be made for cases or reasons that, if available, the right to this erasure may be applied. We also suggest that there should be an exception in the right to erasure of data. This exception, for example, could be in cases where it is compulsory for the data not to be exposed in whatever circumstances, especially, when it is of public interest, or to comply with certain legal obligation, or to establish or affirm legal claims, or submitting legal defense, or for the purposes of scientific and statistical research.

8. We suggest that the Egyptian legislator stipulate the right of the data owner to transfer his personal data to another person, as well as the conditions attached to doing so.

9. We suggest that the Egyptian legislator oblige the officer in charge of data protection and processing to avail the owner of the data with all his personal information at the time of collecting the data. This information must include but not limited to his name, contact details, the purpose for processing, legal basis for processing, recipients and categories of beneficiaries, period for storage of the data, right to obtain a copy of the data, right to modification or erasure or restriction or objection, or right to withdrawal of prior consent to the processing of the data, right to submission of complaints to the Personal Data Protection Authority, source of data (private or public), and whether the data will be transferred to another country. All these information are to be made available to the data owner within a period not exceeding one month from the data's date.

10. The researchers suggest that the appointment of a data protection officer should only be made tolerable by the Egyptian legislator, except in certain special cases or activities deemed necessary for it to be made compulsory, and that it should be specified that it is permissible to appoint a data protection officer from a foreign forensic laboratory, the same way it is specified in the European Regulation for Protection of Personal Data.

Conclusion

In the foregoing analyses, attempt is made to examine the legal aspects of protecting a patient's personal data within telemedicine, by identifying the diverse trends of concept associated with personal data, types of data subject to protection and the importance of protecting them. The study also compares the Egyptian local legislation for protecting personal data in a remotely medical workplace with that of the French counterpart and few other European Nations. The conditions attached to processing of such highly confidential data as specified in the Egyptian legislation, and the rights and obligations arising from such a kind of data

protection, as well as the civil liability that may result from data breach were also clarified to identify the areas that needed to be improved upon. It is, thus, demonstrated that the existence of laws to protect personal data is of paramount importance, more so when the law obliges all institutions and companies to protect the individual personal data that may be held in their possession. The law also makes it compulsory for them to establish internal systems and controls that will process and protect those data. It also gives the individuals concerned, the right to control and monitor the process of data that may be identified with them or collected from them. It, is finally discovered that the existence of law that protects this data will safeguard individuals from blackmailing and exploitation of all kinds, and would be a resilient deterrent to ensure that unauthorized persons or institutions do not use the individual's personal data.

References

Ahmad Saeed, Dirasah Qadhaiyyah. Al-Bayan Newspaper, U.A.E, dated 15/6/2019, at https://www.albayan.ae/across-the-uae/news-and-reports/2019-07-25-1.3613428

Al-Hamm al-Amni wa Huquq al-Afrad: Abhath wa Dirasat. Al-Markaz al-Arabi li al-Buhuth al-Qanuniyyah wa al-Qadhai yyah. Majlis wuzarai al-Adl al-Arab. Jamiat Duwal al-Arabiyyah, Beirut, 2018.

Al-Ittihad Newspaper: dated 27/6/2018; https://www.alittihad.ae/wejhatarticle/99484/%D8

Al-Laihat al-Ammah al-Orobiyyah li himayat al-Bayanat al-Shakhsiyyah, no. 679, Chapter 5, section 44-50, 2016.

Barthélémy Gaillard, Données personnelles: que prévoit l'Union européenne? 16/12/2020, https://www.touteleurope.eu/actualite/donnees-personnelles-que-prevoit-l-union-europeenne.html

Clare Stouffer, https://www.lifelock.com/learn-identity-theft-resources-what-is-data-privacy-and-why-is-it-important.html

Clare Stouffer, What is Data Privacy and why is it Important. 19 January, 2021, https://www.lifelock.com/learn-identity-theft-resources-what-is-data-privacy-and-why-is-it-important.html

Czechoslovakian Regulation for protection of personal data, https://www.uoou.cz/gdpr-obecne-narizeni/ds-3938/p1=3938

Dunya al-Karjati, Amn al-Bayanat wa al-Ma'lumat. 13 January, 2019. https://www.mlzamty.com/search-information-data-security/

Egyptian Personal Data Protection Law 151 of 2020.

Emmanuel D. Jouffin, Présentation du Règlement général sur la protection des données, Hors-série Banque & Droit – mars-avril 2017.

European General Data Protection Regulation (GDPR) 2016/679.

French Civil Law as contained in the amendment of 12th February, 2020.

French Penal Code as contained in the amendment of 5th July, 2020.

https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A31995L0046

https://ico.org.uk/about-the-ico/news-and-events
https://ico.org.uk/action-weve-taken/enforcement//
https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65f
https://www.cnil.fr/fr/la-loi-informatique-et-libertes

Ibn Haydah Muhammad, al-Haqq fi al-Khususiyyah fi al-Tashri' al-Jazaairi: Dirasah Muqarana, M.A Thesis, Universite Ahmed Draia d'Adrar, 2010.

Jean-Philippe Sala-Martin, 2012, https://www.journaldunet.com/ebusiness/le-net/1029637-donnees-personnelles-vers-une-responsabilite-accrue/

Leo Besemer, Why is Data Protection so Important? 11th July, 2018. https://www.exin.com/data-protection/why-is-data-protection-so-important/

Lydia F de la Torre, what is "Convention 108"? Jun 26, 2019, Posted in the following link: https://medium.com/golden-data/what-is-coe-108-3708915e9846

Muna al-Ashqar Jabur and Mahmud Jabur, Al-Bayanat Al-Shakhsiyyah wa al-Qawanin al-Arabiyyah, 2018.

Qanun Himayat al-Bayanat al-Shakhsiyyah: Ta'aziz li al-Haqqi fi al-Khususiyyah am Iham bi tahsin al-Biat al-Tashri'iyyah. Published in the website of Masar Mujtama'in al-Taqniyah wa al-Qanun on 5/12/2020. https://masaar.net/ar/%D9%82%D8%A7%D9%86%D9%88%D9%86-%

The Supreme Constitutional Court of Egypt. Constitutional Case No. 207, dated 1/12/2018. P. 39 at www.eastlaws.com

Toby Mendel, Andrew Puddephatt, Ben Wagner, Dixie Hawtin, Natalia Torres, Global Survey on Internet Privacy and Freedom of Expression, UNESCO, 2012.