International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838; Print ISSN: 2664-682X
Received: 02-11-2018; Accepted: 03-12-2018; Published: 03-01-2019
Volume 1; Issue 1; 2019; Page No. 09-15

Protecting the Privacy of Users of Social Networking Platforms in Light of the Legislation of the Kingdom of Bahrain

Dr. Raed Mohammad Flieh Alnimer
College of Law, Royal University for Women, Bahrain

Abstract
This paper aims to address the users of social networking platforms in regards to protection mechanisms and the various challenges that these users face in attempting to protect their privacy in the online world. It is becoming increasingly recognized that self-presentation in the digital world requires the presentation of the user's personal data, that is due to the fact that the online norm in regards to such phenomena has been shaped in a way which in order to be recognized and given attention to, one must share personal information which results in him acquiring a fan base which is the main goal associated with the participation in such online networks, thus exposing him to various risks. In addition, this paper also tackles another aspect which is related to the use of social networking platforms which is one of the most significant downsides of it, be it the excessive observing of the lives of others, which sometimes reaches the point of obsession, thus resulting in identity crisis issues such as identity theft and impersonation, as well as the extravagant and exaggerated interference of people into the lives of the user whom shares personal information online, which mostly ends in complications, troubles, issues, acts of stalking, or in some extreme cases even crimes. This paper also attempts to demonstrate the concept of processing personal data and determining who is responsible for addressing it on social networking sites.

Keywords: social networking sites, privacy, protection, threats

1. Introduction

As a result of globalization and the constant change in the status of the world in terms of being interconnected and intertwined as a whole, significant developments have occurred in all fields and sectors, and especially in the field of communication and technology. Thus, the economic sector in regards to the business in the market have been exposed to a drastic change in their nature in the sense which traditional commercial channels are no longer heavily used whereby instead they have been replaced by new technological forms. Nonetheless, businesses are in a constant rival position whereas each thrives to be the preceding one in utilizing new and advanced technologies and obtaining information about the public in order to create a customer persuasive policy, in the means of marketing for example. Moreover, with the current movement and direction of the world, it is predicted and very much foreseeable that in the near future all sectors will be engaged in such technological behavior and the traditional channels used previously will be diminished. Thus, businesses must catch up with the modernized phenomena in order to not be left behind and neglected in a world where technology is in a rapid rise and development.

One of these technological developments in the field of communication is social networking platforms and applications, whereby it seems that the service provider of such platforms has a dual role, meaning that these programs not only provide the sole service of entertainment or the benefit they intend to provide, but also collect and store users' personal data and information such as their comments on these webpages, their preferences, personal emails, and all other information that the user portrays on his or her personal page. Consequently, such data is being handed or even sold to companies and individuals whom in their role characterize users based on an area of preference criteria and create groups to be targeted in the sense of for instance pop up advertisements that they shall relate to due to the fact that they fall under their circle of interest.

In addition, it is important to note that users of such social media platforms reveal, by their own free will, information related to their personal life in cyberspace or in the virtual world, in which boundaries are neglected, hence the privacy of users is subject to violation either by the social networking site itself or by other users. In the occurrence of the user portraying his data, whether personal information, images or comments, or other content published, these platforms and through their terms of use signed by the user whom has insufficient knowledge of such matter, save and store all data in their databases. This data can then be made available to users of these platforms according to the settings and conditions of each platform. Ergo, this results in the probability of users' information to be leaked and accessed by other users to the risk of any user accessing another user's data, violating privacy of the former and putting him or her at risk if such data was used unlawfully. Therefore, it is important to protect user privacy at any cost, which is why this occurrence has been widely tackled on both regional and international levels.

As a result of all these transformations that have emerged in our modern world, which led to modern changes that involve new techniques and systems that rely on the computers information technologies, it is highly advisable to educate oneself about these new technologies in the field of information and data exchange (whether through private networks or the internet), as well as the protection of user privacy in regards to social service provider

(personal data and user privacy), and the protection of user privacy against third parties.

Hence, data sharing through online servers raises a list of inquiries to be handled and justified through legislations, such as authoritative body in regards to the data being shared, the geographical boundaries, and conflicts of applicable jurisdictions. Consequently, this subject matter must be addressed through a legitimate framework, in which cybercrimes and violations are handled and user privacy is protected, without prejudice to the fact that in most cases the user himself, through the expression of his own free will, has uploaded his personal data online and exposed himself in the virtual world. That being said, it is necessary to acknowledge the compatibility of existing legislations with the existing occurrences and challenges of the contemporary world, to establish a comprehension of the possible circumstances in terms of violations and protection along with the parallel laws to be applied to them, thus ruling out any loopholes or contradictions, if any.

2. User's Privacy in regards to the service provider of Social Networking Sites

Social networking sites such as Facebook, Twitter, Instagram and WhatsApp are the most popular in today's world, attracting millions of users on a daily basis, not only that but these users also spend a huge part of their day utilizing these sites. Thus, communication between individuals is mainly achieved through such websites, which are seemingly being embedded as a core stone in daily practices and serve as communicating bases which cannot be neglected. These platforms have come to serve as councils or grouped online gatherings and assemblies where ideas, views, perspectives, opinions, beliefs, entertainment, personal information, and even knowledge is shared between users in many forms such as blogs, context, video, audio, photos, etc.

Users of these social media platforms are seen to be somewhat highly attached to their personal webpages in the virtual world, where they can express their views freely and without restrictions or fear of being criticized. In addition, many users hide their identities behind the curtains of the hypothetical world and thus indulge in the strength of being anonymous, meaning they can express their viewpoints freely without the risk of being judged for them. Thus, it is evident that social media platforms have quite an imposing effect whereby they are lodged as an essential part of our daily practices, and that could not be denied.

2.1 Privacy in social networking sites and personal data

The definition of the concept of privacy in social networking sites is one of the most important legal issues that most modern legislations have sought to determine. The importance of doing do so is based on the basic fundamental right of every individual, in this case user of social media, to determine the extent of exposure that his personal data and uploads are exposed to the public. On the other hand, it is also a matter of personal choice and preference to freely choose the mechanisms by which one expresses himself and to share to the extent that he or she wishes to share online. Thus, the users' privacy in regards to their identity such as personal information containing names, addresses, phone numbers, or even preferences, desires, political or social views of users found in their webpages, or stored in a user-shared social networking site can be violated in the sense whereby these data may be hacked into, and then disclosed.

That being said, the protection of privacy in social networking sites is limited to the right of the person to control the information that concerns him, which is one of the most important concepts required by all systems and laws aimed at protecting the privacy of information, and it can be said that the protection of information privacy is the protection of data for individuals who use those sites across the network.

It should be noted that there is a general correspondence between the term privacy of information and protection of data, but not between the sole concept of privacy itself and data protection, whereby the concept of privacy itself concludes a wide range of meanings and segments when interpreted; it is a general concept, from which privacy of information emanates from. Moreover, due to the increased use technology, the concept of privacy of information has become a significant contemporary topic, which could not be neglected.

Referring to Bahrain Personal Data Protection Law No. 30 of 2018, personal data or data is defined as "Any information in any form of an individual, directly or indirectly identifiable, in particular through their personal identification number or one or more of their formal features of physiological, intellectual, cultural, economic or social identity. In the determination of whether an individual is capable of being identified, all means used by the Data Manager or any other person, or which may be available to them, shall be taken into consideration".

Also, sensitive personal data is defined as: "Any personal information that directly or indirectly discloses the ethnic origin of the individual, their ethnic group, political or philosophical views, religious beliefs, trade union affiliation, criminal record, or any data relating to their health or sexual status.

Consequently, it is clear that the user is the main persona of the social media networks, and as defined by the jurisprudence: a person who joins a network and surfs the internet in order to obtain or broadcast information. This definition combines both aspects that the user indulges in whereby he can be the one receiving and benefiting from information or entertainment, or at other times can be the one providing such information of entertainment to other users, utilizing these platforms to share for instance ideas and pieces of work such as literary works as a means of self-marketing, or publishing to the public. In such scenario, the server/platform provider is merely the supplier of the shelter that users consolidate in, in which through it they share whatever they choose to on the internet.

The user of the social networks is required to be a natural person not less than a certain number of years specified by the communication service provider, nor should he be convicted of a crime of sexual assault or other crimes against honor unless he is rehabilitated, in accordance with the terms of membership of the network, which vary from site to site. It is also required by these social networks to acquire the user's acceptance to comply with the policy of use of personal data, and submit his personal data at the time of registration in the network, which later on will be used for commercial practices by the service provider which stores in their data bases all information in regards to their users.

It should be noted that the protection of data and personal information is applicable whenever is is subject to a specific person or at least a person can be determined through the data stored and accessed by him, thus if it is related to an anonymous

person and the data submitted is false and does not lead back to the identity of the user, then the protection of privacy shall not be validated since there is no real risk of any privacy violation.

Moreover, the submission of false personal data by users online when registering with the networks results in complications law enforcement in cases whereby crimes or violations occur online due to the hustle of obtaining proof of the real identity of the violating user. It is not easy, given the nature of social networking sites, to find a solid solution to this problem, although it does not negate the technical developments in this regard, which depend on the IP address of the computer to locate it and then thus later identify the user of the network.

Therefore, there is a high possibility for users of social networks to be below the age range specified by these networks and that is due to submitting false information regarding their age, in violation of the membership requirements. In this case, the bearer of the user's responsibility for his or her harmful actions will fall on their legal guardian's, or for instance if the harmful act conducted by the minor took place in a computer lab at school, the supervisor or teacher in charge at the time of the occurrence may also be held liable and bear the responsibility along with the guardians. That is, of course, based on the general rules of law in regards to harmful acts conducted by those lacking legal capacity.

Accordingly, social networking platforms have the right to suspend any user's account or webpage where false information has been submitted or processed, or where harmful or disrespectful information is being posted and shared. Thus, these platforms have the competence to filter their webpages in order to make sure that all users are complying by the rules and regulations of the network as well as respecting the public order that is to ensure that their online community is a user friendly platform which is free of violations. The acts of suspensions are either by the network's supervisors own motion or based on suggestions and complaints of other users that is after making sure of the validity of the complaint.

2.2. Processing of personal data

After demonstrating the concept of privacy and personal data, one must clarify the details of these data and the conditions for their processing and therefore determine who is responsible for such conduct.

2.2.1. The concept of personal data processing

Processing of personal data means " Any process or set of operations performed on personal data by automated or non-automated means, including the collection, recording, organization, classification, storage, modification, amendment, restoration, use or disclosure of such data by broadcast, publishing, transferring, making available to third parties, merging, blocking, wiping or destroying them".

Based on the previously stated definition, it is seen that the sole act of collecting personal data itself is not prohibited, however the act of collecting personal data through illegal means and ways is prohibited. Social networking sites collect and store three types of user-generated data which are, personal data, internet connection data, and browsing data related to the sites which the user browses and encounters. Therefore, social networking sites collect, record, save, store and perform any other operations on personal data that the user places on the site all fall under the concept of processing personal data. Thus, it is important to shed light on the fact that illegal data collection only occurs when the data is collected illegally, and not submitted by the user himself by his own discretion and free will.

2.2.2. Conditions for processing personal data

Patently, data processing may not be conducted without the consent of the author of such data and his free will. This consent must be free of any vices, specific for the collection of the data itself, and subject to the knowledge and awareness of the author in regards to the purpose of collecting it.

As a matter of fact, speaking of Facebook which is one of the most important and influential social networking sites, its consent policy contains three aspects: free consent since the user submits his data with his own free will, specific consent because the user particularly responds to certain a certain set of questions and has the choice not to respond, and finally that the user expresses his consent by accepting the terms and conditions of the website. However, the user may not be aware of the purpose of collecting such personal data requested by the website's information department, which may be used for commercial purposes without the knowledge of the former, to the benefit of the latter.

Due to the precise nature of such data processing, the server provider is in a position whereby he must handle such data in an upright and ethical manner and save them for the intended purpose of collecting needed information for the sake of the wellbeing of their websites, and not for any hidden reasons such as leaking the information for commercial purposes.

2.2.3. Identifying who is responsible for processing personal data in social networking sites

In this important to reflect upon the bearer of the responsibility of processing data in social media sites, in order for user to ensure his or her right to fair compensation in regards to what is published of his personal data without his knowledge or consent. In other words, the user must comprehend who is responsible for the leakage of information so that he can question the fault and have a base for compensation.

Referring to the Bahrain Personal Data Protection Law of 2018, the data manager is defined as "A person who decides, individually or in association with others, the purposes and means of processing certain personal data. Where such purposes and means are established by the Law, the person responsible for the processing shall be the Data Manager. In the other hand define the data processor as "The person who processes the data for and on behalf of the Data Manager. This does not include everyone working for a Data Manager or Data Processor".

Through the above definition and the practical aspect of implying it, one could my perceive that the management of social networking site is the one solely responsible for data processing, as the main purpose of the existence of the law itself is to protect the rights and freedom of individuals from violations of their privacies.

In addition, as denoted in the Law of Telecommunications in Bahrain, which states in Article 23 "The Director General and employees of the Authority shall not disclose to third parties confidential information received directly or indirectly in the performance of his or her functions, and this prohibition shall apply after leaving office or position", it is indicated that there is an obligation on the service provider to respect the privacy of the messages and communications of its users, which extends to the

social networking sites. The concept of communication comprises any means of sending or receiving symbols, signals, letters, writings or pictures.

In addition, the legislator stressed the importance of protecting private data, evident in Article 75 of the Bahraini Telecommunications Law which stipulates "Without prejudice to any more severe penalty stipulated in the Penal Code or any other law, a fine of not more than 10,000 dinars [1]. Sending any message informing the sender that its content is false, misleading, contrary to public order or public morals, or that may endanger the safety of others or affect the effectiveness of any service. Relating to the content of any message or its sender or sender, unless Be eavesdropping or disclosure under the authorization of the public prosecutor or an order issued by the competent court".

2.2.4. Use of personal data for advertising purposes

It is clear that the user data is an important financial resource for social networking sites, whereby they sell such data to companies and whom categorize these users and send them sponsored advertisements which fit their preferences and taste which can be concluded through the user's data. The most effective data that aids in the categorization is the user's age, gender, social status, place of residence and personal interests, all of which are personal data, subject to collection for personal data processing requirements.

For example, Facebook, in exchange for the free access of its server by users, analyzes user data for marketing purposes, whereby advertisements or advertising guidance is based on the data collected and grouped based on similarities. In accordance with the site's privacy policy, this action is committed not to disclose the identity of the member or to display his data to others, but just through the site to collect information and analyze interests and directing all of this to advertisers, without disclosure of specific user's information but only as a general data base.

Thus, it is concluded through the above explanation that the site records any activity carried out by the user in the server, and then collects all the information related to this activity, and provides advertisers, who either direct the ads to the user or not, depending on the level of similarity between the user's preferences and the item advertised for. These advertisements are based on the communication of the advertiser to the site to gather target consumers in terms of age and place of residence and gender as well as personal interests and all data that fit the advertisement, and then the site displays the text of the correspondence and the link to the advertiser on the pages of members whose personal files correspond with the target consumers of the advertiser. Finally, the ad is sent or displayed to the target users and the latter can view the ad by clicking on the ad banner.

Notwithstanding the fact that users might benefit from such targeted advertisements that fall under their area of preferences and wants, such data collection also has an obvious downfall which is related to personal freedom as these ads help to create profiles of internet users in categorized groups without the latter's knowledge nor their consent, and thus the user's personal data is handled as commercial goods between sold and used to the benefit of social networking sites and advertisers.

On the other hand, in terms of advertising, Facebook for instance created a system which demonstrates the products of websites automatically on the personal pages of users who dealt with these sites previously. Technically, this system is based on the implicit consent of the user to participate in it, which means that the user is subscribed by default to see such ads on his page, unless he explicitly "un-subscribes" by clicking on the set phrases to "not see this ad again" for instance. Thus, technically Facebook argues that it gives its users a choice and that they are being exposed to such ads by their own choice.

3. Protection of the privacy of users against third-party

As a general principle, the Bahrain Civil law in its branch governing the liability for personal acts states that: "Any fault that causes harm to third parties is required to be compensated."[1] And: "The person shall be liable for compensation for damage caused by his wrongful act," [2].

The above-mentioned article depicts that the principle of compensation in regards to any fault committed is set as a general matter thus it covers all rights whether financial rights, moral rights or personal rights. Any fault must be compensated, no matter what type of fault or if intentional or not. Thus, there is no doubt that the social networking sites are one of these fields in which the user has privacy rights, and any violation to such right privacy results in the right to compensation to be paid by the violator.

3.1. The extent to which privacy is protected on social networking sites

There is a real fact that the digital revolution led us to a time of revelation, which is associated with the most important human right, be it his personal privacy, which has become a place of interest and target of a lot of users of modern technologies, whether in good faith or bad faith. However, despite the risks accompanied with such conduct, the social networking platforms have seen a growing demand from users, who are eager to publish and share many information on their websites including their personal information, which is quite the new trend nowadays to publish their day to day practices on personal blogs.

One of the most controversial issues is the emergence of new technologies in the field of telecommunications, resulting in many legal conflicts which have a negative impact on the growth of these servers due to the problems they faced after the introduction of new technologies. As a matter of fact, the main issue in accordance to the new technological aspects added is that users can identify other users and have access to their personal information. For example, users can identify others through mutual friends in some websites and networks, or through phone number or email, which a form of violation of privacy is since personal information of can be accessed without the permission of the author.

It is clear that the rapid transition to the use of information and communications technologies and the growing technical transformations have not allowed for effective compliance with risks, whether by governments and policy makers, or by individuals. Over the past two years, the world has produced unprecedented levels of data, surpassing the entire human history, which has alerted those in the public and private sectors to the importance of effective management, taking into account the technical, economic, administrative and legal aspects of

[1] - article 158 Bahrain civil law.

[2] - article 159 Bahrain civil law.

ensuing, with the transition to digital, data has become invaluable and a resource for the knowledge economy. Thus, the whole world has become interconnected and somewhat dependent on the internet and online world in many fields and commercial practices.

However, the number of people using the Facebook network is more than 2 billion, up to 800 million using Instagram, and more than 1 billion on WhatsApp. The data generated by this usage exceeds 2.5 Exabyte approximately one minute. Instant Chat applications are another source of data production, with more than 527,000 images being sent by Snapchat, per minute, and Linked in more than 120 new accounts, Twitter users sending 456,000 Twitters, Google has more than 3.6 million searches, Amazon earns more than three hundred thousand dollars of sales, which are carried out in one minute online, as well as for the huge volume of investments that countries make in the field of large data.

These enormous figures explain the direction of large corporations towards investing in personal data where it is a wealth of companies, both technical and traditional, to use in product development, advertising, analysis, analysis of natural persons' preferences, needs, consumer habits, and interests.

In contrast, the flow of information on the Internet is increasing as the number of connected devices and the variety of storage devices, such as hard drives and cloud computing systems, vary, and the applications that are engineered depend on how they are developed and used to provide services. Note that most of the data collection occurs without the knowledge of the person concerned.

In this context, the concept of privacy must be defined so that it can be known that individuals control the extent, timing and circumstances of sharing their lives with others. Privacy intervenes as a right exercised by the individual to limit the exposure of others to aspects of his or her life, which may be personal thoughts or statements and a description of the protection of personal data of the individual, which is published and circulated through digital media. Personal data is the e-mail, bank accounts, personal photos, work and housing information, and all data we use in our online interaction while using the computer, mobile phone, smartphone, electronic board, etc.

Thus, it is evident that it is necessary to define privacy in social networking sites as the right of the individual to decide for himself when and how and to the extent to which information can reach his or her users or others. Thus, it is clear that everyone has the right to protection from interference in his or her affairs. It is also a right to freely choose the mechanism by which the user expresses himself, his wishes and actions to others on social networking sites [3]

Privacy in social networking sites, in its simplest sense, is related to the privacy of users of these sites, in regards to the facts or information they place online via their personal computers or smartphone, or stored in their email or on a social networking site that may be compromised such as mail theft or abuse is a violation of privacy, as well as electronic espionage, or intercept messages sent via email for the purpose of knowledge, or knowledge of the contents, and then disclosure of the secrets that may contain such messages, Such as political, social, health and other violations and breaches according to Article 26 of the Bahraini Constitution law which states that : "The freedom of postal, telegraphic, telephonic and electronic communication is safeguarded and its confidentiality is guaranteed. Communications shall not be censored nor shall their confidentiality be breached except in necessities specified by law and in accordance with procedures and under guarantees prescribed by law" [4].

The protection of privacy in social networking sites is limited to the right of the person to control the information that concerns him, which is one of the most important concepts required by all systems and laws aimed at protecting the privacy of information, and it can be said that the protection of information privacy is the protection of data for individuals who use those sites across the network. The user can avoid the availability of personal information for all by limiting the disclosure of this information to certain users only such as friends on his webpage whom he chooses to allow to share content with.

It is important to note that privacy is different from security. However, breaking security means unauthorized access to protected codes or user data and information. For example, a social network may be a victim of piracy or a virus, but if the attack does not result in exploitation for personal information the privacy here is protected from infringement.

The violation of privacy is derived from unauthorized access to information that is of a private nature, and may be constituted as a result of a security breach. For example, some social networking sites where users may have agreed to submit their personal data to academic researchers, marketing companies, security institutions and others in accordance with their profitability. Finally, it can be said that social networking sites are a risky substance in regards to privacy and security, and are prone to be targeted to have their security breached in order to reach a large number of user information.

In general, privacy is a non-objective measure, which differs from one society to another, depending on the customary norms of each area and the mindset of the members of each community. Thus the concept of privacy is constantly changing to adapt to the circumstances of the time and place where it is interpreted. However, the common idea that is universally taken into consideration is that privacy a basic fundamental human right and each individual has the right to its own privacy and for it to not be violated by any means.

3.2. User role's (infringed) in violation of privacy

There is no doubt that every person has his personal freedom, and he is the only one who decides to disclose through his own will his personal information. Thus, whenever one decides to disclose personal information about his life and affairs to the public by making these data available on online servers to everyone without limitation or choice, he will have the biggest role in attributing to his privacy being violated by others and his information being leaked to the public, due to his own actions.

Allegedly, some social networking sites, including Facebook, send user warnings about rights and responsibilities, stating explicitly that when a user publishes content or information using

[3] - Mahmoud Abdel Rahman Mohammed, 2010, The scope of the right to private life, comparative study of positive law (American - French - Egyptian) and Islamic law, Dar al - Nahda Arab, p. 77.

[4] - See Article 26 of the Constitution of the Kingdom of Bahrain and its amendments for the year 2002.

the "public" settings, this allows everyone, including non-users of the site access to and use of information [5].

As a matter of fact, it seems necessary that the privacy policy for social networking sites include some guidelines for site users on how to deal with personal information of third parties who have published their data and raise awareness about the rightful and wrongful conduct. It is necessary to say that the user concerned must have the right to object to the processing of his or her personal data, and also refuse the use such data in commercial studies and research without being provided with a justification or reason, along with a choice to either accept or deny such request. Everyone has the right, in principle, to decide how to use their data, refuse to include it in certain electronic files or choose to transfer it to third parties. Accordingly, this right is evidently expressed and exercised by the act of refraining from answering the questions that are related to personal data during the data collection process, which is usually the time of registration in the website. Furthermore, the user may exercise this right to request the removal of his data from files with commercial objectives.

The rejection at a later stage, through communication, is responsible for processing, sending email, or otherwise, without incurring any cost, and the official must answer within a time limit prescribed by law. He cannot invoke the lack of clarity of the request or any other excuse; he is supposed to refer to the applicant and request clarifications or information necessary to build a response. If the person responsible for processing rejects the request, otherwise, the applicant may, in this case, review the relevant authority or bodies responsible for the protection of personal data [6].

Herein, everyone is entitled to request that his or her personal data be corrected, supplemented, blocked or erased when such data is incorrect, incomplete, inappropriate, outdated, or essentially processed, such as sensitive data. It is the duty of the person in charge of processing, when the request is legitimate, to initiate the requested process. In accordance with the principle of the legality of data, it is not possible to allow the processing of personal data on social networking sites, unless the person concerned has been obtained or necessary to implement a legal obligation to which the person concerned is a party or to perform a legal obligation or A task of public interest, performed by the person responsible for the processing, or by the body to which the information was given or which is necessary to carry out the legitimate interest of the person responsible for the processing or of the person to whom the information has been delivered and which does not result in damage to the fundamental rights of the person concerned.

In general, all applicable laws, in the area of privacy protection and confidentiality of information, permit the collection and use of data, within certain limits, based primarily on the consent of the person concerned. This can make the phenomenon of data collection and data processing online somewhat acceptable, due to the fact that the boundaries set give an impression of some kind of control to the person concerned. However, the reality is quite far from that, since these websites give their users the illusion that they are in control of what is shared and that everything is done based on the user's will and concept, but contrarily the practice that really occurs is that the data of these users is benefited from for commercial and marketing reasons which have no relation to the intended purpose of the user disclosing his information online. The Internet user rarely reads long terms items that are submitted to him for approval before giving him the right to use the social networking program, which means that the consent he gives is not the result of a correct will, but a result of an act of being naïve and uneducated in this topic.

In fact, through practices that have been adopted to this day, consent can be demonstrated in a number of ways, whether through written expression or indicated by an act or behavior, depending on the circumstances. Some service providers require the user to click on the "I agree" button to express his consent to a number of terms and conditions, while others refer to the mere use of the Site, or the application, as consent, to hidden terms and conditions, provided for, somewhere in the Site, and all such means may create a binding legal relationship, which is known as the contract, according to the law.

The user in social networking sites, overwhelmed by a lot of information when opening an account, is not obliged to search, prospect, find these terms and conditions, or to see the privacy policy. Most users of social networking sites do not read the terms and conditions of use, which appear on the screen. They often fail to understand the quality of personal data that they are asked to agree to disclose, address, and do not have the ability to take note of the details of the treatment and their impact on them, whether they agree to the terms of use of social networking sites or when they click the consent button.

Most users of social networking sites cannot expect modern technologies, artificial intelligence capabilities, and many different, sometimes complex, possibilities for processing personal data. Leaving aside the complexities of contracts that are presented to them, where all the details and information are given about how the data is processed and used, these contracts are submission contracts which means that the user has no option of rejecting unless he decides to abandon the use of the communication site.

Although in most legislations in general, the definition of contracts and their components, and the conditions of their validity, it is considered that in the contract between two persons, there is a first-party offer, acceptance by another party or several parties with the intention to create a legal obligation, legal capacity to enter into a contractual obligation, free will, Thus, the validity of the contract is affected by any form of coercion, false declaration, or unconscious consent. Accordingly, any approval by clicking the "I agree" button, or agreeing to the social networking agreement, lacks understanding, full understanding, and explicit consent. Moreover, the will in this case may suffer from an unacceptable agreement when the user cannot discuss or modify the terms and conditions of use.

When it comes to smart devices, where the consent of the person concerned is required, it becomes more complicated to use a number of applications, in unclear technical ways, to exchange data between two different applications, or to pull out a list of friends and addresses. It is also worth noting that the person concerned has become a source of personal data, not of his own, but of his family, friends, acquaintances, and possibly his clients.

[5] - Ashraf Jaber Sayed, Legal aspects of social networking sites, and privacy problems, op. Cit., P. 89.

[6] - Sameh Mohamed Abdel Hakim, 2007, Internet Crimes on Persons under Bahraini Legislation, Comparative Study of Egyptian Legislation, II, Dar Al-Nahda Al-Arabiya, Cairo, p.30.

4. Conclusions and recommendations

It is important to know how many users think that in the time of social networks he has created a digital world for himself. He travels through it with a virtual identity, interacting with who he wants and as he wishes without being seen by the other. However, one may not be ignorant or ignore that these networks, in their own view, are imposed by the laws of use and their conditions, which push them to formulate proposed social relationships in a different digital context than the real ones, but are proposed by friends and who can include them in the list of friends, it drives us to get to know our friends and friends friend. Therefore, it is a highly complex network that weaves digital relationships based on its goals and objectives.

Ergo, the spread of social networks and the excessive use and time of the day spent by the user on the internet, so created a state of complacency in the individual privacy, and over time exceeded the traditional sense of privacy, which was about the private life of the user and ensure control over information that wants to inform others, in the right to do so, to make the user's private life material for publication and participation with others, where private information became more abundant for both companies and individuals.

When a user accesses any social networking site, he accepts terms and conditions that he has consciously or unconsciously authorized to sell or display his personal information and data, especially demographic and polarized by the advertisers, which expose him to violating his privacy, despite the promotion of these networks through the "privacy policy" on the site, which can automatically snoop the user and make him convinced and assumes that his information is safe when following the privacy policy steps offered by these sites.

To conclude, it is important to shed light once again on the fact that the privacy of the user of social networking sites continues to dissolve due to the exposition and revelation of such data, which is being subject to violations and risks oscillating between violation and risks for commercial benefits, by being used in advertising and marketing and creating categorized data bases and targeted audiences for each advertisement and each group of users with similar preferences and circumstances. Thus, in order to protect oneself from such violations, one must pay great due diligence and care in what is shared and disclosed by him online, because what is published today can have a great impact later on.

Finally, I recommend the following:

First: The necessity of subjecting the social networking sites while processing the data to common technical and legal rules so as to effectively guarantee the privacy of the user.

Second: The need to find a specific mechanism on the social networking sites to show the user and alert him to the seriousness and importance of settings, which helps the user to secure his account on social networking sites by adjusting the privacy settings on the site to determine the scope of privacy on his account. These settings allow him to choose between setting his data to all or all friends or some friends, and to avoid showing, controlling, correcting, or deleting data on search engines if necessary.

Thirdly, the importance of proof of social networking sites, as the distinction between the special character and the public nature of a Facebook page is to respect the privacy settings that the user selects for his page, and therefore the special nature of this page disappears, the privacy of the page allows anyone to enter. There would then be no grounds for violating the confidentiality of correspondence placed on the wall of this site.

Fourth: The existence of social networking sites everywhere and at all times, and the size of the personal information contained in these sites makes it a rich source of evidence of possible proof, and given the nature of these sites, it raises significant challenges, some of them credibility of the evidence obtained from these sites. Based on the above, competent agencies should look for ways to collect information that would confirm the credibility and authenticity of the evidence.

5. References

1. Ashraf Jaber Sayed, Legal aspects of social networking sites, and privacy problems.
2. Sameh Mohamed Abdel Hakim. Internet Crimes on Persons under Bahraini Legislation, Comparative Study of Egyptian Legislation, II, Dar al-Nahda al-Arabiya, 2007.
3. Mona Al Ashqar Jabbour, Mahmoud Jabbour. Personal Data and Arab Laws: Security Concern and Individual Rights, Arab Center for Legal and Judicial Research Arab Council of Ministers of Justice, League of Arab States, First Edition, Beirut, Lebanon, 2018.
4. Mahmoud Abdel-Rahman Mohamed. The scope of the right to private life, comparative study of positive law (American - French - Egyptian) and Islamic law, 2010.
5. Mohamed Sami Abdel-Sadiq. Social Networks and the Violation of the Right to Privacy, Dar Al-Nahda Al-Arabiya, Cairo, 2016.
6. Mohammed Hussein Mansour, Electronic Responsibility, New University House, Alexandria, 2003.
7. Mohammed bin Eid Al-Qahtani. Protecting the personal privacy of users of social networking sites. Law, College of Criminal Justice, Naif Arab University for Security Sciences, Riyadh, Saudi Arabia, 2015.
8. Mahmoud Abdel Rahman Mohamed. The scope of the right to private life, comparative study of positive law (American - French - Egyptian) and Islamic law, Dar al - Nahda al – Arabiya, 2010.
9. The Constitution of the Kingdom of Bahrain amending the year, 2002.
10. Law No. (30) For the year, 2018. issuing the Personal Data Protection Law Date: 19/07/2018 Official Gazette No. 3375.
11. Decree-Law No. (48) For the year promulgating the Telecommunications Law in the Kingdom of Bahrain, 2002.
12. Bahraini Civil Law o, 2001.
13. Bahraini Penal Code of 1976 and its amendments for the year, 2018.