How to verify the contracting person through electronic means

Safaa Nageh bin Higab Hamid
PhD researcher Minia University Faculty of Law
Email: drsafaanageh@gmail.com
Under the supervision of
Dr\ Jamal Atef
Professor of International Law Minia University

Abstract:

In spite of the ease in dealing with electronic dealings and its widespread availability, especially in previous years, the topic increased its importance after the emergence of the new Crohn virus, which highlighted the effective role for electronic transactions in the entire international community, and it is worth noting that the risks of epidemics and diseases have raised many problems during The last twenty years, the most important of which are problems of a legal nature, passing through the SARS epidemic in 2003, then the HINI epidemic in 2009, or the EPOLA epidemic in 2014, and finally the CORONA epidemic, which is the most widespread as it represents a global crisis.

Which made electronic transactions not a entertainment or even an optional method, but it is the only available means under the current circumstances, and one of the most important problems raised by the contract is how to verify the personality of the contractor, which does not raise any problem in the traditional dealings due to the physical presence of the parties, which we lack in dealing with Then, so that transactions can be carried out in a safe and effective manner that guarantees the seriousness and sincerity of transactions, away from any fraud or fraud.

So we will review the most important points that ensure the verification of the personality of the contractors, which is summarized in privacy via the Internet, including images of the attack on personal data, then we are exposed to the sources that threaten the privacy of personal data, and through the efforts and means used to protect that data, whether in international or Arab legislation, and finally the effects Liability resulting from the assault on personal data.

This study aims to several objectives, as shown below:

1- A brief presentation on the meaning of the right to privacy and exposure to the most important images of the violation of the right to privacy that affects contracting through social media.
2- What data requires legal protection?
3- The sources that threaten the privacy of personal data, so that each contractor through these means can protect its data from plagiarism and theft.
4- The methods used to protect personal data.
   A- In documents or in international legislation.
   B- In Arab legislation and constitutions.

Study methodology:

This study is mainly based on the analytical approach and the comparative approach.

Key words: The right to privacy, the personal data of the electronic contractor , , Request to stop assault, tort.

Introduction :

If verifying the identity of the contractor is easy in the traditional contract for the availability of the physical presence of the two parties, it is not possible in the electronic contract, since it is done through an open network (the Internet), which makes it difficult for the contractors over the Internet to prove the actual presence.

The matter has further complicated the general situation that has swept the international community with the emergence of the new Corona virus, which has made electronic dealing an indispensable necessity, whether at the level of individuals in the same country or on a scale beyond that .....

So it was necessary to research how to verify the person of the remote contractor, who is considered the first problem with the electronic contract, which is part of my PhD, in order for the contract to take place away from any fraud.

In the context of talking about how to verify the identity of the contractors, we are exposed first to privacy via the Internet, then we deal with the mechanisms used to protect the privacy of people's data and finally we are exposed in some detail to

the implications of proving responsibility for violating personal data in four sections:

The first section; Online privacy

Violation of privacy via the Internet is considered an apparent criminal phenomenon in which the alarm bells are ringing, to alert societies to the magnitude of the risks and the tremendous losses caused by computer crimes that aim to attack the data in its technical significance in its wide technical significance These crimes are committed by smart criminals, who possess the tools of technical knowledge, aiming to undermine the right to information, which may reach all stored computer data and information transmitted through information systems and networks, as it touches the private life of individuals and threatens national security and national sovereignty, and loss of confidence in dealing across The Internet (**Hoome, 2016, p. 245**), which threatens the giant edifice of transactions resulting from electronic contracts in various fields.

Now we are exposed to the definition of the right to privacy, then to the most important images of violating privacy that affect online transactions:

First: Definition of the right to privacy

It is the ability of an individual or people to isolate themselves or information about them and thus they express themselves in a selective and selective manner.

Second: Pictures violating the right to privacy

In the Egyptian legislation, privacy and the protection of personal data did not receive adequate attention, as the Egyptian constitution suffices to note the state's commitment to protecting private life, whether for individuals or companies, as it stipulated that "private life is inviolable, and it is inviolable. For postal, telegraphic, and electronic correspondence," And phone conversations And other means of communication are forbidden, and their confidentiality is guaranteed, and it was not permitted to be confiscated, viewed, or censored except by a causal judicial order, for a specified period, and in all cases specified by law. Or to stop it or to deprive citizens of it arbitrarily, and the law regulates this. ”(**Egyptian Constitution, 2019, Article 57)**

This was approved by the Supreme Constitutional Court, "and as well as above, there are areas of private life for each individual that represents invasions that

cannot be accessed and should always be considered and for a project not to be invaded by anyone to guarantee its secrecy and the preservation of its sacredness and a motivation for attempting to hijack it or to embezzle some of its aspects and a special aspect of Through modern scientific methods that have reached an amazing extent, and the growth of their penetration capabilities has had a far-reaching impact on all people, even in their most accurate affairs and related to the features of their lives, and even with their personal statements that have become familiar with them and their plunder of their eyes and ears, and often have access to them. For the embarrassment and harm of its owners and these areas is one of the characteristics of life and its intruders. They protect two interests that may appear separate but complement each other, as they relate in general to the scope of personal issues that must be kept confidential, as well as the scope of independence of each individual with some important decisions that are - in view of their characteristics and effects - more related to the insight and influence of the life situations that I choose their patterns and the crystallization of these areas All of them - which the individual turns away from, reassuring their inviolability to resort to them away from the tools of control and their tools - the right to have a private life bordering them in a manner that takes care of intimate ties within their scope. While some constitutional platforms do not decide this right with an explicit text in them, but some are considered to be the most Bore rights and broader, which is also deeper in connection with the values advocated by civilized nations (**Supreme Constitutional Court, 1995, Case No. 28/16 BC constitutional)**

And when the legislative structure was devoid of a special law that protects the confidentiality of personal data for individuals in the Egyptian law, we had to search in the French law, which had a precedent in the field of protecting personal data, where a law was issued to protect and process files and personal data for individuals on January 6, 1978[1], then the law was amended No. 801 of 2004[2], and finally was modified by Resolution No. 25 of 2007[3].

[1])Loi n° 78-17 du 6 janvier 1978 relative à l' informatique,aux fichies et aux libertés,.dit loi Foyer

[2])Loi n° 2004 – 801 du 6 août 2004 relative à la protection des personnesphysiques à l'égard des traitements de données à caractére personnel et modifiant la loi n° 78 – 17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, J.O, 7 août 2004, et disponible sur.

[3]) Décr. n°2007-451 du 25 mars 2007 modifiant le décr.n° 2005-1309 duoctobre 2005 pris pour l' application de la loi n° 78-17 du 6 janvier 1978 relative à l' informatique,aux fichies et aux libertés,modifiée par la loi n° 2004-801 du 6 août 2004.

The French legislator has expanded the definition of personal data in the second article of Law No. 801 of 2004, concerning the protection of personal data, where it came. "His personal number or by reference to anything license."[4]

With this expansion adopted by the French legislator in the concept of personal data, we find that it has included any information that could identify any person in a direct or indirect way, because narrowing the concept of personal data may allow many entities to infringe upon it, especially with the advancement of personal data collection techniques, which Many entities are allowed to encroach on them, especially with the advancement of data collection and sharing techniques, Data distributed with different databases may not indicate the identity of the person per se, but if linked it may reveal the identity of the person.

Based on the foregoing, we find that we are facing a lot of images that violate privacy in its broad sense, but what we are exposed to are the images that affect the field of contracting via the Internet, which relate in particular to the personal data of the contractors and that affect the extent of the contractors 'confidence so that the contractors can verify the identity of each of them. The personality evolved with the development of the Internet, so the name, surname and mailing address are no longer available, but rather increased and diversified to include the person's image and voice, his premium over another set of data related to his financial ability, behaviors, habits, inclinations, tastes and most of all the data that relates to The human body "biometric data:"[5]

---

[4])) "Toute information relative à une personne physique identifiée ou qui peut être identifiée ,directement ou indirectement,par référence à un numéro
d' identificationou à un ou plusieurs éléments qui lui sont propres .Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont disposeou auxquels peut avoir accès le responsable du traitement ou toute autrepersonne."

[5]) (Environmental data) is the one that depends on knowing whether these materials are not applicable based on the formal, physiological and anatomical characteristics of each person such as cornea and fingerprint.
Look:

1. Defense Science Board (DSB) (September 2006). "On Defense Biometrics" (PDF). Unclassified Report of the Defense Science Board Task Force. Washington, D.C.: Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics: 84 seen in . ٢٠ February 2010
2. "Biometric Identification". Communications of the ACM, 43(2), p. 91–98. doi:10.1145/328236.328110 – saved in ٠٧ November 2012In Way Back Mission website .
3. ^ Bill Flook (3 October 2013). "This is the 'biometric war' Michael Saylor was talking about". *Washington Business Journal*.. Archived on 9 July2018

Look :
https://ar.wikipedia.org/wiki .

1- Assault on name and surname:

The right in the name to preserve its name is one of the rights inherent in the identity, and therefore it is characterized by the characteristics that characterize those rights that do not accept disposition, and do not accept inheritance after death, and the inability to statute of limitations. It is the official means of identifying individuals **(Sultan, without publication year, p. 220**)

According to what the law says, "Every person has a surname, and the surname of a person is attached to his children." (Egyptian Civil Law, 1984, 38)

The name and surname are considered one of the most important personal data through which an electronic contract can be defrauded, since the name - whether it is the name of a natural or legal person - is the distinctive sign for him that gives the customer confidence in dealing or not, so a person needs a name, whether it is a real name or the name of his choice For itself to be encountered in electronic transactions and one of the most important uses or applications in which the name appears clearly, via the following Internet:

1- Longing online, entering through websites and virtual shops via networks such as Amazon or Alibaba and others, requires writing the name to conduct the desired electronic transaction.

2-Create e-mail, through sites that provide this service, such as sites that provide this service, such as the Yahoo, Hotmail, Google, and other multiple uses of the same mail after its creation, such as sending messages, and holding negotiations to buy or sell goods and others that we will talk about In detail in the next lines .....

3- Create personal accounts (accounts) on social networking sites, the most famous of which are Facebook, Twitter, MySpace, and other sites through which private correspondence and political and social views are exchanged, as well as many different electronic transactions. (**Al-Tohamy, 2001, 390**) - (**Othman, without publication year, pp. 9-10)**

2 - Assault on e-mail: -

E-mail is considered one of the most important means of electronic contracting, as it is the ideal tool for transferring and storing files that contain personal data. It is not permissible to attack or monitor it, nor to reveal its content except with a license from the judiciary, and communications via the Internet in general are subject to the principle of electronic confidentiality that must be

respected by individuals And governments alike, and this is what made sure to confirm international constitutions and laws.

3-Infringement on electronic payment cards: -

The electronic contract needs to implement fulfillment by paying by credit card and fulfillment card, and this process is required for the customer to record its details with what it contains of information and data such as the customer's balance, creditworthiness and the amount of his income, even data that relates to his previous financial actions and is undoubtedly considered as private information Confidentiality in his personal life, and the danger does not stop only in being a violation of the privacy of personal life, but it can be exploited, analyzed and classified by the bank or the merchant who deals with him in this way while fulfilling his financial obligations, due to what he reached M modern and technological development, allowing tremendous information to the bank easily , This exposes the personal life of individuals to infringe upon the consent of the owners

Therefore, this personal and financial information of the persons must be kept strictly confidential and limited only to the customer and the merchant within the limits of the debt settlement subject of the contract, and this is available in the electronic money payment system, especially the electronic money wallet payment system, where it allows the person to keep the transactions confidential and the buyer's confidentiality, but These methods are not the best choice as they are not desirable by the official authorities as they fear clandestine transactions for criminal reasons related to combating money laundering crimes.

4- Attacking the phone number and car number:

Finally, it should be noted that the phone number of a particular person is considered as personal data, especially with the advancement of technological means, as it has become one of the fastest means of communication between the contractors, whether it is a home phone or a mobile phone.

As well as a person's car number, such as personal data, as it is not permissible for a person to attribute it to himself out of fraud or impersonating the owner of the car number to gain the confidence of the contractors with him (**Gadeed, 2012, p 269-271).**

We see that what has been mentioned in the previous items is examples of some personal data, as it is difficult to limit personal data under certain items, so any information that relates directly or indirectly to a specific natural person has an identity or can identify an identity, and any information that can be performed to make inclination Consumption is subject to blackmail, or makes it vulnerable to impersonating a person and contracting with a name is considered as personal data that must inevitably have the necessary legal protection, but the difference between personal data must be emphasized and Privacy, personal data are not all subject to privacy, for example, any information about the individual's general activity constitutes personal data but does not fall under his private life, the personal data that is the focus of our study is that which relates to the individual's private life, and which he does not wish to disclose, then the right In defending privacy, it is not new since it is from the nineteenth century, but with the spread of information technology, the need to provide protection for personal data has emerged as well.

The second section

Sources threatening the privacy of personal data

The use of e-commerce applications raises many problems regarding the availability of legal protection for the contractor. The spread of data through social media networks through entering on social networking sites that can provide their users 'personal data to the user's audience, as well as an area for collecting personal information via the Internet The person's recent visits to the sites before entering the desired site, so it has become a challenge to protect the personal data provided by the person, whether before or during the process of concluding the contract, from viewing it to non-contracting persons Wish she manipulation, Among the most important challenges that must be provided with the necessary legal protection, just as access to personal data can take place indirectly, and we take for that the most important of these methods:

First: Collection of personal data through the use of Internet technologies: -

This is done through the use of individuals or entities for a specific type of protocols called communication protocols via the Internet. Communication through this network between computers is not done through the use of standard protocols.

The protocol called **TCP / IP**[6] can be used to transfer large amounts of data and information between Different computers, and consists of identifying each machine used by what is called an **IP** [7]address, but as for the information on the web pages it is stored by the HTML language, and finally it is transmitted via the HTTP protocol, and by using such protocols, its users can register the personal information of those who use their data to browse the Internet, and this data can be recorded by those who provide communication via the Internet. **(Azan, 2013, p. 2)**

Second: Collection of personal data through cookies technology COOKIES: -

It is text files sent by the server of the site that the user visits over the Internet to the user's device's hard disk, as it maintains a copy of the user's data such as the Internet IP address, the sites the user visits frequently, and the data that the user needs to enter to enter On some sites such as entry form like name, email, credit card number, etc. ....

In spite of the ease that we provide this technology for the user when entering again for the same site where the site maintains a copy of the cookie file inside the server for it makes the user do not need to enter this data again, the cookie technology facilitates the user to quickly access the sites that he previously visited,

[6]) () It is an abbreviation of Transmission Control Protocol // Internet Protocol "It was invented in 1970 and was part of the research" DARPA ", which has connected different types of networks and computers. Funding this institution was public in order to develop this "language", and therefore it is characterized by its lack of affiliation with anyone, and the result is that it has become a public domain, and therefore no one can claim the right to use it only for him. Moreover, the "TCP / IP" protocols consist of hardware and independent software programs. Therefore, anyone can be connected to the Internet and share information using any type of computer. The protocol is for the computer., On the Internet is a set of rules that define how computers can communicate with each other over the network they are on. The protocol describes the manner in which these devices must exchange messages and transmit information. The protocol varies according to the type of service provided by the network. For example, the Internet is based on a set of protocols that are one family is TCP / IP. TCP / IP is actually two different protocols but they always work together in the Internet system, and for this reason they are accepted to be described as one system
Check it out: **https://www.thaqafnafsak.com/2012/05/tcpip.html**

[7]) Internet Protocol address, which is a logical digital address assigned to each computer, printer, adapter, router, or any other device that is part of the TCP / IP network, and the IP address is the primary component on which a structure is built Networks: Where there is no Internet without an IP address, it is an address used to uniquely identify each node in the network, and it links the World Wide Web to each other.
Check it out: https://mawdoo3.com/_IP

but The danger of having such data on the user's device as well as stopping on the sites that the user frequent makes the user vulnerable to knowing behavior and inclination, and what he likes and what he hates, and what he specifically wants, which is what the advertising and advertising sites are adopting until the user is directed to the type that comes from Basket , One of the first companies in this field is **Doubleclick**[8] **.**

Third: Losing personal data: -

One of the most dangerous ways in which personal data can be used in a way that represents a danger to the user is the loss of data, and one of the clearest examples of this is what happened in one of France's companies in 2006 where the company lost a cylinder on it for the personal data of nine thousand workers in it, and recently it caused a wrong configuration process An online database has exposed the personal records of most of Ecuador's residents, including children, while what is the largest diversion in Ecuador's history, according to the **ZDNet** website, and the database was discovered by security researchers at **vpnMentor**, which contains nearly 20.8 million User, It is a number greater than the total population of the country, according to that it includes the data of the deceased persons, and the most comprehensive data was the civil registry data of the Ecuadorian government, as the base contains the full names of citizens, dates of birth, places of birth, home addresses, state A and identification numbers Patriotism, and lots of information. The data in the family index - which includes information about each family member's family, such as children and parents - allows anyone to rebuild family trees for the entire country's population, It includes information about each citizen's family members, for anyone rebuilding the family trees of the entire country's population, and the database is up to date, as it contains up-to-date information until 2019, including records of the president of the country, and even Julian Assange, who previously obtained asylum The

[8])Click Interprice is a pioneer company in the software industry. The company is located in a distinctive location in the heart of the capital, Cairo, and it includes the departments of Marketing, Sales, Technical Support, Programming, Quality Control, Customer Follow-up Department, Financial and Legal Management and a store for the company in addition to a factory to produce the program.
See:
https://www.doubleclick.com.eg/home.

politician is from the small country in South America, with a national ID number granted, and the database also contains information about children some of whom were born this spring, with 6.77 million records for children under the age of 18, including children's names, national identity numbers, Places of birth, gender, and also contain J records with abbreviated names of private entities, such as (**BIESS**)[9] and (**AEADE**[10]), including 7 million financial records, and 2.5 million records containing details of car and vehicle owners. (**Al-Tohami, 2011, p. 407**)

The third section; Means of protecting the personal data of the contractors

The world is witnessing a huge technological revolution, during which the importance of means of communication is increasing day by day, especially the Internet, which ranked the most important in the transfer and exchange of information.(**https://www.iweb123.com)**

First: The means used to protect personal data in international documents and legislation:

The idea of protecting personal data has been incorporated in the documents developed at the international level and in international legislation, and has evolved in a way that suits the tremendous technological development that occurred recently ...

It is one of the most important documents developed at the international and regional levels, which have had a definite impact in drafting the legal system for the privacy of personal data.

• What is stated in Article 12 of the Universal Declaration of Human Rights issued on 10/12/1948 AD: "No one shall be subjected to arbitrary interference in his private life or in the affairs of his family, his home, or his correspondence, nor for

[9]) (BIESS) denotes the bank of the Ecuadorian Social Security Corporation, and contains financial information for some Ecuadorian citizens, such as account status; account balance; credit type; and information about the account holder; including job details.

[10]) (AEADE) stands for Association of Automobile Companies of Ecuador, and contains information about car owners and their cars, including models; and auto license plates.

campaigns that affect his honor and reputation. Everyone has the right to be protected by law." Such interference or campaigns. "

• Also stated in the text of the International Convention on Civil and Political Rights dated 12/12/1966 CE, as stated in Article 17 thereof.

a. No one shall be subjected arbitrarily or unlawfully to interference with his privacy, family affairs, home or correspondence, nor any unlawful campaigns that affect his honor or reputation.

B. Everyone has the right to the protection of the law against such interference or attacks. ".

• The European Directive also stressed in several directives the principle of protecting the personal data of the consumer via the Internet.

• As well as the European directive issued No. 97/66, which relates to the treatment of data that are personal and protect the private life of users of wireless communications, which was amended according to the European directive No. 2002/58, which relates to the treatment of data that are personal and protect the private lives of individuals in the framework of electronic communications

• The 1967 Stockholm Conference, which defined the right to a private life as the right to be a free person and allowed to live as he or she desires, with minimal interference to the outside, with specificities

• The 1968 Tehran Human Rights Conference, which was extremely important to focus attention on protecting personal data from the dangers of digital technology.

• The specialized study developed by the Council of Europe on the protection of personal data in European countries and the first decisions it issued to protect the privacy of this data (1973 and 1974)

• The guide (1980) developed by the Organization for Economic Cooperation and Development, which includes guidelines that affected European countries, members of the organization, and the Council of Europe, which developed the 1981 agreement (a global agreement on protecting data from the risks of automated processing)

• The United Nations' 1990 Guide

• The 1995 European directive on protecting data and regulating its flow across borders

Western countries were also concerned with enacting laws to protect personal data, such as the American Privacy Act (1974), the French law relating to the protection of automatically processed data (1978), and the Protection Act

British Data (1998), British Human Rights Law (1998) and others

(https://www.lita-lb.org/archive/56-questions-answers-- protection-of-personal-data-html)

Finally, the European GDPR "Protection of Information and Privacy" Law came into effect on May 25, 2018, which is a real step in the world of privacy protection, and the first draft of this law appeared in 2012 out of fear of the penetration of American technology companies, especially The Big Four (Java), Google, Amazon, Facebook, and Apple in European markets and in the lives of Europeans.

It is worth noting that this law has preceded conflicts and discussions, and was approved by the European Parliament in 2016, where the last update of data protection laws was 1995, and it was emerging at a time when there is a real need for new legislation to keep pace with this development, especially after the recent Cambridge Analytica and Facebook scandal.(**https://www.france24.com**) .

The Wyze leak information scandal was discovered days before the end of 2019.

(**https://www.youm7.com**)

Second: The means used to protect personal data in Arab legislation:

As for the Arab countries, they dealt with the issue of legal protection of personal data in many Arab constitutions. The Constitution of the Arab Republic of Egypt stipulated in Article 57 of the current constitution - after the amendment – that "Private life is sacrosanct, and it is inviolable".

Postal, telegraphic, electronic, telephone conversations, and other means of communication are inviolable, and their confidentiality is guaranteed, and they may not be confiscated, viewed, or censored except by a reasoned judicial order, for a specified period, and in the cases specified by law.

The state is also committed to protecting the right of citizens to use public means of communication in all its forms, and it is not permissible to arbitrarily suspend, stop, or deprive citizens of them, and the law regulates this.

Likewise, the Egyptian constitution stipulated the necessity of protecting the information space and considering it as part of the national economy of the state.

Article 31 stipulated that "information security security is an essential part of the economy and national security system, and the state is obligated to take the necessary measures to preserve it, as regulated by law."

The Qatari constitution stipulated in Article 37 the inviolability of human privacy, and in the Tunisian constitution that established the right to privacy in Article 24 of it, which was unique in defining personal data, while the Western constitution focused on the side of protecting communications in addition to protecting the right to privacy, and the text of the constitution The Algerian woman is forbidden to violate the private lives of citizens in Article 39 of his rule, as he considered that the private life of natural persons is a basic right, the law punishes for its violation, and the Libyan constitution stipulates in Article 42 that private life has its sanctity, and it is forbidden to interfere in it in any form except with the permission of the judge The specialist.

Likewise, the Lebanese constitution stipulated in its introduction that it adheres to the international agreements on human rights, without the slightest distinction between its children, as well as it was considered that respect for public rights and freedoms is one of the most important pillars of the Democratic Republic.(**gaboor, 2018, p 26-27)**

The fourth section; The effects of liability resulting from the assault on personal data

Civil liability is considered the most appropriate sanction, whether resulting from violating rights and freedoms or breaching obligations in the Internet world,

because resorting to criminal responsibility requires confirmation of the principle of criminal legitimacy, which requires criminalizing existing violations across the Internet, as there is no crime and no punishment except with a text, and given Because the virtual world has its own nature and the speed of its development and the multiplicity of images of violations that are difficult to imagine within it and determining penalties for them, and therefore the asylum of the injured person to civil liability is the best choice as it is not required for its emergence that the violation be erased Again, on the part of the legislator, and those who have been assaulted on his personal data are entitled to ask the court to stop the assault on his data, along with a right to compensation, and we will take them accordingly.

First: The injured person's right to stop assaulting his personal data

The injured person has the right to resort to the judiciary to stop the assault on his data, and this has been explicitly stated in Article 50 of the Egyptian Civil Law. "

According to the previous article, the aggrieved party can resort to the judiciary to stop the attack on a right to privacy and consider it a right of the person, so that he enjoys the same protection inherent in his character. **(Al-Ahwany, without publication year, p. 145**)

The French Civil Code also stipulated the same principle with regard to the protection of the right to privacy in Article 9 of it, as in the first paragraph of which it stated, "Everyone has the right to respect his private life", and the second paragraph of the same article indicates that the court has the right, and without prejudice to the right to compensation, To order temporary measures to prevent the continuation of the violation of privacy, the right to protect privacy has been the main driver for the development of the idea of protecting personal data since entering the era of computers in the years 1970-1980, where the transition to the digital age, the active role of users and the focus of control over the flow of information and its exploitation, whether from Before private entities or APR D have special interests (**Moyse , 2018 , p14)**

Second: The right to compensation

The person affected by the attack on his personal data has the right to demand compensation for the damage caused by this attack, and the establishment of responsibility in such a case is based on tort liability in accordance with the text of Article 163 of the Egyptian Civil Law, "Every mistake causing harm to others who commit the compensation"

The act of assault is the responsibility - the default error -, and for the right to compensation to arise, this error will cause harm to others, and the default error will be achieved upon the breach of one unchanging legal duty, which is the obligation not to harm others. **(Al-Sanhuri, 2006, p. 509)**

And the default error has several forms, including collecting personal data without the consent of the owners, using personal data for commercial purposes, penetrating personal accounts and intending to defame and blackmail their owners.

As for the intended harm to the liability arrangement, it is a condition that dictates the idea of civil liability itself, considering that it is its job that, since its separation and its distinction from criminal responsibility, is compensation for the damage. **(Abdel-Al, 2008, p. 5**)

The damage is not limited to the material damage that has been inflicted on the human person, such as the loss of a legitimate financial right, or the seizure of commercial secrets, but the concept widens to include moral harm that affects a person's feelings, emotions, and dignity, such as that inflicted on a person by publishing abusive images of him or defaming his reputation or insult and slander.

We cannot fail to mention in this regard that, except that if the presence of the injured person has the right to demand compensation for damage to a period, this harm must have been achieved, by the fact that it has already occurred as a video posting responsible to a person in front of the public through social media, or damage will occur Inevitably in the future, such as disseminating commercial information about a person's activity through social media, despite its removal by court ruling, this does not prevent some competitors from keeping copies of them.

If compensation is due to harm to the quality of reality and the fact that it is falling, it is also necessary in case of missing an opportunity, such as what a person does by posting pictures on one of the social media for his girl in a drug abuse situation, and it turns out that it is a false image that has been installed by one of the computer programs that Used for this purpose, however, the publication of these images led to the end of the engagement of this girl, which missed her opportunity to marry.

Finally, the emergence of responsibility is necessary for a causal relationship to exist between error and damage, so the error must be what caused the damage, which is the relationship of causation. (**Al-Sharqawi 1991, 527)**

The assessment of compensation is subject to the judge of the matter, without high control from the Court of Cassation, whenever the reasons arise, and there was no binding text in the law that followed certain criteria regarding it.

According to the principle, the estimate of compensation is given the value of the damage at the time and occurrence, except that the judiciary is down to practical considerations that are the missed opportunity on the debtor, which is to deliberately prolong the dispute, to take advantage of the low currency value, so the amount of the compensation amount is determined by the value of the damage at the time of the judgment Compensation **(Lotfy, 2013, p. 61)**

Finally….

From the foregoing, it is clear that the protection of personal data has become a priority for the attention of countries, where every day huge amounts of data appear electronically, which requires the necessity of providing strict laws to protect them from abuse by others and their use in illegal ways.

Results and conclusions:

1- Criminalization of any data collection without the owner's permission.

2- Every person's responsibility for securing the personal account against penetration.

3- The evidence of the assault on the data results in the right of the aggressor to request the cessation of the assault on the one hand, and to claim compensation on the other hand.

Recommendations:

1- An Egyptian legislator must put in place legislation to protect personal data, similar to the French legislator.

2- The purposeful media in the state should take a course in educating users of the Internet of the danger of giving their data, and the damages that may befall them as a result of excessive use of this data.

References

١- Abdel-Al, Muhammad Hussein, 2008, Estimating Compensation for Variable Damage, "A Comparative Study", Arab Renaissance House, Cairo.

٢ - Al-Sanahuri, Abdel Razek, 2006, Part One, Bar Association edition.

٣- Al Sharkawy, Jamil, 1991, The General Theory of Commitment - Sources of Commitment, Arab Renaissance House, Cairo.

٤- Al-Ahwany, Hossam El-Din Kamal, without publication date, the right to respect for private life, the right to privacy, "a comparative study", Arab Renaissance House, Cairo.

٥- Al-Tohamy, Sameh Abdul Wahid, 2011, Legal Protection of Personal Data, Kuwait Law Review, No. 3, pp. 390, 407.

٦- Azan, Amin, Protection of the personal data of the electronic consumer, Economy and Consumer Magazine, publisher Shams El Din Abdani, Volume 5, Issue 6, published June 2013, p. 2.

٧-Bill Flook (3 October 2013). "This is the 'biometric war' Michael Saylor was talking about". Washington Business Journal Archivé de l'original le 9 juillet ٢٠١٨.

٨-"Biometric Ide"Biometric Identification". Communications of the ACM, 43(2), p. 91–98. doi:10.1145/328236.328110 Une copie enregistrée sur la Wayback Machine le 7 novembre٢٠ 12 .

٩-Bill Flook (3 October 2013). "This is the 'biometric war' Michael Saylor was talking about". Washington Business Journal Archivé de l'original le 9 juillet ٢٠١٨.

١٠-Defense Science Board (DSB) (September 2006). "On Defense Biometrics" (PDF). Unclassified Report of the Defense Science Board Task Force. Washington, D.C.: Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics: 84 Consulté le 20 février ٢٠١٠.

١١-Gadeed, Fathi, 2012, Protection of the right to privacy during contracting online, Law Magazine, No. 3, page No. 265, 269, 271.

١٢- Hemme, Layla, 2016, violating morals and privacy via the Internet in Moroccan legislation, Tangier city, Morocco.

١٣- Jabbour, Mona Al-Ashqar / Jabbour, Mahmoud, 2018, personal data and Arab laws, Arab Center for Legal and Judicial Research, Council of Arab Ministers, League of Arab States, first edition, Beirut.

1٤- Lotfy, Hossam, 2013, The General Theory of Commitment, Book Two, Al-Ahkam, Cairo .

1٥-Nathalie MALLET-POUJOL, 2007,protection de la vie privée et des données à caractére personnel, étude disponible sur, la date de mise en ligne est: mai.

١٦- Othman, Abu Bakr Othman, responsible for assaulting the personal data of social media users, Tanta, Cairo.

1٧-Pierre Emmanuel Moyse , 2018 , Le droit au respect de lavie privée “les défis digitaux, une perspective de droit compare , Canada .

١٨- Sultan, Anwar, without publication date, General Legal Principles, New University House, Alexandria.

Constitutions

1- The Egyptian Constitution .

2- The French Constitution.

3- The Qatari constitution.

4- The Tunisian Constitution.

5- The Algerian Constitution.

6- The Libyan constitution.

7- The Yemen constitution.

Websites

1- https://ar.wikipedia.org/wiki .

2- https://www.thaqafnafsak.com/2012/05/tcpip.html.

3- https://mawdoo3.com/_IP.

4- https://www.doubleclick.com.eg/home.

5- https://aitnews.com. .

6- https://support.google.com/mail/answer .

7- https://www.iweb123.com .

8- https://www.lita-lb.org/archive/56-questions-answers--حمايـة-البيانـات-الشخصـية-html .

9- https://www.france24.com .

10- https://www.youm7.com .

الملخص:

بالرغم ما توفره التعاملات الإلكترونية من سهولة فى التعامل وإنتشارها بكثرة خصوصاً فى الاعوام السابقة ، إلا أن الموضوع زادت اهميتة بعد ظهور فيروس كرونا المستجد ، والذى أبرز الدور الفعال للتعاملات الإلكترونية فى المجتمع الدولى بأكملة ، وجدير بالذكر أن مخاطر الأوبئة والأمراض قد أثارت العديد من الإشكالات خلال العشرين عام الأخيرة وأهمها المشكلات ذات الطابع القانونى ، وذلك مروراً بوباء SARS عام ٢٠٠٣ ، ثم وباء HINI عام ٢٠٠٩ ، أو وباء EPOLA عام ٢٠١٤ ، وأخيراً وباء CORONA عام ٢٠٢٠ والذى يعتبر أكثرهم إنتشاراً حيث أنه يمثل أزمة عالمية .

مما جعل التعاملات الإلكترونية ليس وسيلة ترفية أو حتى وسيلة إختيارية ولكنها الوسيلة الوحيدة المتاحة فى ظل ظروف الحالية ، ومن أهم المشكلات التى يثيرها التعاقد هو كيفية التحقق من شخصية المتعاقد والذى لا يثير أى مشكلة فى التعامل التقليدى نظراً للوجود المادى للأطراف ، والذى نفتقده فى التعامل عن بعد ، وذلك حتى تتم التعاملات بشكل آمن وفعال يضمن جدية وصدق المعاملات ، بعيداً عن أى غش أو تدليس .

لذا سنقوم بإستعراض لأهم النقاط التى تضمن التحقق من شخصية المتعاقدين والتى تتلخص فى الخصوصية عبر الإنترنت مشتملاً على صور الإعتداء على البيانات الشخصية ، ثم نتعرض للمصادر التى تهدد خصوصية البيانات الشخصية ، ومروراً بالجهود والوسائل المتبعة لحماية تلك البيانات سواء فى التشريعات الدولية أو العربية ، وأخيراً آثار المسؤلية الناتجة عن الإعتداء على البيانات الشخصية .

أهداف الدراسة :-

١-عرض موجز لمعنى الحق فى الخصوصية والتعرض لأهم صور إنتهاك الحق فى الخصوصية التى تؤثر على التعاقدعبر وسائل التواصل الإجتماعى .

٢-ماهية البيانات التى تستوجب الحماية القانونية .

٣- المصادر التى تهدد خصوصية البيانات الشخصية حتى يتمكن كل متعاقد عبر هذه الوسائل من حماية بياناتة من الإنتحال والسرقة.

٤-الأليات المتبعة لحماية البيانات الشخصية .

أ- فى الوثائق أو فى التشريعات الدولية .

ب- فى التشريعات والدساتير العربية .

٥- الجزاءات المترتبة على الإعتداء على البيانات الشخصية للغير.

منهجية الدراسة:

تعتمد هذه الدراسة بشكل أساسي على المنهج التحليلى والمنهج المقارن .

النتائج والإستنتاجات :

١- تجريم أى تجميع للبيانات بدون إذن صاحبها .

٢- مسؤلية كل شخص عن تأمين حسابة الشخصى ضد الإختراق .

٣- يترتب على ثبوت الإعتداء على البيانات حق المعتدى فى طلب وقف الإعتداء من جهة، والمطالبة بالتعويض من جهة أخرى .

التوصيات :

١- يجب على المشرع المصرى أن يضع تشريع لحماية البيانات الشخصية، أسوة بالمشرع الفرنسى.

٢- يجب على الإعلام الهادف فى الدولة أن يقوم بدورة فى توعية المستخدمين للإنترنت بخطورة الإدلاء ببياناتهم ، والأضرار التى قد تصيبهم جراء الإفراط فى إستخدام هذه البيانات .

الكلمات الداله: الحق فى الخصوصية ، البيانات الشخصية للمتعاقد الإلكترونى، طلب وقف الإعتداء ،المسؤلية التقصيرية .