RES MILITARIS
REVUE EUROPEENNE D ETUDES EUROPEAN JOURNAL OF MILITARY STUDIES
Social Science Journal

Applicable Law in personal data disputes on the Internet

By

Assist. Prof. Khatam Abdul Hassan
Legal Management Techniques Department, Najaf Technical Institute, Al_Furat Al_Awsat Technical University, 31003 Al-Kufa, Iraq.***Corresponding author**: Khatam@atu.edu.iq

Abstract

Most network management is in the United States of America, so it is difficult for them to introduce all state legislation associated with such networks, subjecting disputes in the network to their laws by concluding a user contract with the network user who, when agreeing to transfer all of its data to the United States of America and accepting it to submit to its laws, has several caveats, particularly with regard to the legality of the terms of use and privacy policies that process personal data. for the user, without having any responsibility to manage the network. In order to find an acceptable legal formula, we found it necessary to establish a law applicable to the protection of personal data that was flexible and reasonable.

keywords: networks - user - law of will - personal data.

Introduction:

Social networks are part of the internet, which is characterized by its international standard, as it provides a service that transcends the boundaries of natural states and different nationalities, in which digital content that is personal data entered by the user of the network when creating accounts, and then publishing and circulating information successively, or be works of art, industrial, commercial and literary, which are displayed and published on the sites of communication, and therefore if there is an infringement of personal data, or intellectual property, there must be a legal description to provide protection for them, and the application of a law to settle disputes that arise.

The importance of paper:

Perhaps the most prominent feature of networks is the personal user data the subject of the research as they themselves publish them with details of their own lives, this data must be preserved to a minimum, as personal data is a personal right of human beings, the privacy of users is now the most important topic of concern to the world, and it is looking for solutions to resolve its disputes within the scope of private international law.

Problem of the paper:

Personal data on the Internet is not erased from the network, but is archived in a huge database, and remains preserved even after it has been erased by the subscriber. Many networks have begun to invest such data for commercial and non-commercial purposes, thus infringing personal data, especially since the terms of use include explicit provisions for the acquisition and use of data, without taking any legal responsibility for doing so, posing the problem of determining applicable law to settle disputes using such data, and obliging networks to assume legal responsibilities to maintain and use such data only in appropriate legal forms.

Questions about the paper:

How is the applicable law on personal data defined within the rules of private international law? If there were rules that could be applied, was they compatible with the Internet? What is the legal basis for requiring the management of communication sites to submit to those rules? So we try to answer these questions, by dividing the research into two demands, the first is the application of personal law, and in the second the application of the law of will.

Personal law enforcement

The rule of submission of matters relating to the personal status of the natural person, whether it be nationality law or home law, is an established rule of private international law.(1), Since personal data is part of the civil status, it means that it is also subject to personal law, but this rule faces difficulty in applying the Internet, which does not recognize geographical boundaries or the nationality of users, and since personal data on the Internet does not exist to date, some States have developed national legislation to protect their citizens on the Internet in the face of management policies, networks, and such legislation, European legislation, so we try to do so. Requirement - To indicate the extent to which personal law can be applied on the Internet, by dividing it into two branches, the first section deals with the content of personal law, and then the basis for its application, as follows:

Content of personal law

In this section, we show the content of European Guidance No. (46/95), and then the principles contained in the Safe Harbor Programme, as follows:

First: European Guidance No. (46/95): (2), The European Guidance aims to provide protection for personal data, while ensuring the principle of free data transfer between European countries only, and guarantees a range of fundamental rights for users of the network, as well as disputes over who collects and processes information.

A. Fundamental rights of network users: these rights are:

1 The right to object, the user has the right to object - when legitimate reasons are available - and refuse to process his or her personal data.
2 Access to information, i.e. the user, once his or her identity has been established, has the right to require the personal data processor to access his or her information and to request that it be corrected whenever necessary.
3 The right to be forgotten (3). That is the user has the right to request the data processor to erase personal data that he or she does not wish.

The right to respect the purpose of the treatment, i.e. to collect information with the consent of the user and the objectives of his project. (4)

Data processor obligations include:

Declaration: i.e. obtaining user satisfaction and informing them when collecting their personal data, explicitly and transparently.

Information: The user must be informed of the mandatory or optional nature and the identity of the persons to whom the collected data will be generated.

Confidentiality: The data processor must take all technical and legal means to protect such data.

The content of the Safe Harbor program: includes several principles that the data processor must adhere to, which are somewhat in line with the principles of European guidance, namely:

1 Obligation to notify the user when collecting and using his personal data.
2 The obligation to give the user the right to decide whether or not to publish his personal data.
3 The obligation to obtain the user's consent when transferring their data to a third party and giving the right to object to it.
4 The obligation to give the user the right to modify his personal data.
5 The obligation not to transfer or modify the personal data of a third party that does not adopt the privacy protection policy.
6 The obligation to maintain the confidentiality of data through a security system against penetration. (5).

The basis for the application of personal law

In this section, we try to lay the groundwork for the application of personal law on the Internet, to which hundreds of states relate to each of their own personal data protection legislation, thereby demonstrating the effectiveness of such legislation and the extent to which it is binding on the Network, as follows:

The basis for the application of personal law:

It is well known that the Internet does not recognize geographical boundaries, i.e. there is no home law or nationality law because of the international nature of the network, yet the efforts of States to find possible legal and technical solutions must not cease, and we believe that the application of personal law can be based on one of these criteria:

1. The criterion for protecting public order: public order in the methodology of conflict is a protective character based on the exclusion of the application of foreign law when it violates public order, as well as the public order preventive status, which is called laws of immediate application that enjoy the status of public order, preventing them from entering into any dispute with any other foreign laws. (6) The European Union, for example, has given exceptional importance to personal data in accordance with binding legal rules, as we shall see it, so it can be said that the basis for the application of personal law is based on the fact that the protection of such data falls within the rules of immediate application, which are characterized by the applicable public order.
2. Safe Harbor Program Standard: A technical standard, which is a self-regulating method whereby the United States Department of Commerce verifies the obligation of internet company officials to respect the principles and rules of the program in providing protection for all personal data when transferred outside EU countries. (7)

It can therefore be said that the basis for the application of personal law is based on a technical standard, the Safe Harbour Programme, as this programme is a European legal rule (European Guidance No. 46/95) applied in the European Union which we explain in the subsequent section obliging companies operating on the Internet to respect the personal data of EU citizens.

Second: How effective is personal law in requiring internet networks to protect personal data:

The question of personal law enforcement, based on the standard of protection of public order, or the safe harbor programme standard, may seem relatively easy in theory, but it is not in practice, for the following reasons:

With regard to the standard of protecting public order, it may run counter to the lack of acceptance of the Internet, as hundreds of States are connected to the Internet, each with its own culture, as what is considered to be an infringement of personal data in one State, the freedom of expression of opinion in another State may be different, as the idea of protecting public order is different according to state cultures.

Moreover, a few countries have developed national legislation to protect personal data, including the European Union and Canada, while many countries connected to the Internet do not yet have national laws in the protection of personal data. (8)

The Safe Harbor program standard is limited, as Facebook and Google have joined it, while many networks have not yet been regulated, including Twitter and MySpace, and the program only includes the personal data of EU citizen users and cannot be applied to the rest of the world. (9).

Therefore, the basis for the application of personal law may run counter to the lack of acceptance of the Internet - it can be accepted in a narrow scope at the EU level and therefore does not establish a disciplined general rule in personal data disputes.

Implementation of the Law of Will

By origin, the law governing contractual obligations is the law determined by the common will of contractors. Although most legislation agrees on this asset, it is difficult on the Internet, as employment contracts are monopolized by the network's management, and if it is left to individuals to appoint the law applicable to the contract, there is an agreement on the appointment. Since use contracts and privacy policy in networks are compliance contracts, the user can only approve them, how is the law of will adopted in this case, we try to clarify two issues, the first being the employment contracts, the privacy policy and the conditions that pre-determine the applicable law, and then show how the basis for the application of the law of will in the settlement of personal data disputes, so we try to indicate in this requirement the extent to which the law of will can be applied in the Internet, by addressing its content in the first branch, and by explaining the basis in its application in the second section, as follows:

Content of the Law of Will

When a person is using any network, it is necessary to register online, which includes a technical and legal procedure, which is to fill a set of minds, and then click the follow-up button, and then agree or reject it. As long as a person wants to register, they are forced to press the agree button. These technical procedures are entirely within the employment contract and privacy policy. We will therefore show this as follows:

First: Employment contract: The employment contract constitutes a contract of acquiescence, because the user has no discussion, modification or partial rejection of certain terms of the contract, and once approved when pressing an agree button, the user is fully

consenting to use. (10) When reviewing most of the terms of the network contract, we find a provision referring to the application of California law.(11) most networks are American, for example, the Facebook network, which states in article (17) disputes: "Any claim, cause of a claim or dispute between us and you shall be resolved from the offences of using this statement, Facebook or associated with it, exclusively in the California State Court, and regardless of any conflict in the Qur'anic texts, agree to submit to the jurisdiction of the State of California, by imposing a decision on all such claims."(12), The YouTube contract also stipulates in Article 14 (14) that (terms of service are subject to the internal substantive laws of the State of California, regardless of its conflict with the principles of the laws, and any claim or dispute of service determined exclusively by a competent court located in Santa Clara County (California).(13)

From the foregoing, it is clear that the provision to define the applicable law within the terms of the employment contract.

Second: Privacy Policy: Registration on any network requires approval of the employment contract, as well as approval of a privacy policy that contains several items, including the personal data clause, and when referring to facebook's privacy policy, it is explicitly determined to possess personal data by saying (giving us all the rights necessary to enable your app to work with Facebook, including the right to use the content and information it provides us in the form of data flows, diary and user procedure events). (14) Other networks also indicate that personal data is owned. Article 18 of the Facebook employment contract refers to (... Agree to transfer your personal data to the United States and process it there). (15)

The basis for the application of the law of will:

The basis for the application of the Law of Will in personal data disputes on the internet is the user's acceptance of the use contract and privacy policy, as the contract of use is a contract that sets out the rules and conditions for the use of the website regulated by the networks. (16) When the use of the network is approved, the user agrees that all his personal data be transferred and processed to the United States of America for use in several fields - if the personal data trade is considered a future trade. (17) As some see it, the law applicable in conflict is California law, so the state of privacy breach according to the above data is in the opinion of jurists.(18) It's possible, because it is based on the user's prior consent to the use contract and privacy policy, and with the user's consent to the contract, is the applicable law when disputes over personal data occur in the network, so when the user agrees to the privacy policy, it is an acceptance of the use of personal data, whether he or she has the knowledge, - which is extremely dangerous yet remains a legally sound basis, regardless of the fact that the contract of use is a contract of compliance remains a valid and binding contract. There can be no conceivable dispute over the definition of applicable law although it is very dangerous in terms of determining the legal and judicial competence in favour of network management, which may not meet the protection of the weak party (user), especially since the terms of the contract are written in English that may not be fully understood, or approved without reading the terms .

Conclusion

After completing our research on applicable law in personal data disputes on the Internet, we can draw conclusions and suggestions as follows:

Conclusions:

1 Knowledge is the basis for protecting personal data, as a person should be careful with the data he or she publishes on the Internet.
2 Traditional rules of private international law cannot resolve disputes over personal data on the Internet, and despite the efforts of States, solutions are still insufficient because of the dominance of the management of certain networks by imposing their powers and jurisdictions, which requires an international convention to establish a unified support rule applicable to the network specialized in the protection of personal data with a technical control mechanism, as the law is integrated with technology in this regard.
3 Most use contracts and privacy policy do not include determining liability for network management in the event of a breach or unlawful use of personal data owned by network management, which is extremely dangerous.

Suggestions:

1 It is necessary to activate the right to forget, which includes erasing all personal data that the user does not wish to remain stored and subject to indefinite trading, as it may at some point be disseminated information without awareness or subsequent remorse.
2 If network management is a legitimate breach of personal data based on the use contract, that contract must be amended to put an end to the responsibility of network management to maintain such data.
3 Legal rules must be established that are recognized at the international level, such as european guidance that includes the protection of personal data by giving the user the right to know and correct when using his or her data.

Automated software within the network that erases personal data after a reasonable period of time should be organized automatically to achieve the legal security of the user.

References

Charbel, W. Q.: Internet Law (Digital Content of Social Networks): C6, Human Rights Publications, Lebanon, 2013.
Tony, M, I. Legal Organization of the Internet, I1, Publications issued by Publishers, Lebanon, 2001.
Amer, M. K.: Conflict of Laws, C1, I1, Culture Publishing and Distribution House, Jordan, 2010.
Abdo, J. G.: Lessons in Private International Law, I1, Majd University Foundation for Studies, Publishing and Distribution, Lebanon, 2008.
Youssef, H. Y., Electronic Commerce and Its International Legal Dimensions, I1, National Center for Legal Issues, Cairo, 2011.
Tarek, J, S. R.: Legal Protection of The Privacy of Personal Data in the Digital Age (Comparative Study), Research published in the Journal of Law and Economics, Supplement to Issue 92, Egypt.