ISBN 978-967-11350-4-4

"RIGHT TO AUTOMATIC DELETION OF DATA IN THE ELECTRONIC ENVIRONMENT VS THE PRIVACY LAWS OF MALAYSIA"

Dr. Manique Cooray
Faculty of Law
Multimedia University, Jalan Ayer Keroh Lama, 75450, Malaysia

Gita Radhakrishna
Faculty of Law
Multimedia University, Jalan Ayer Keroh Lama, 75450, Malaysia

Mohd Emir Feizal bin Mohd Fakhrunnasri
Faculty of Law
Multimedia University, Jalan Ayer Keroh Lama, 75450, Malaysia

ABSTRACT

The increase in storage and processing capacities enable information concerning an individual to circulate within the network, even though it may no longer be valid. This makes the current principle of accuracy and proportionality of data obsolete. "Obvilion" could mean an obligation to delete data, but could equally refer to a prohibition to futher use the data. If the specific problems of Internet media and social networks are focused upon "obvlion" could also amount to the prohibition to further disseminate the data.

Firstly, this paper focuses on the right to automatic deletion of data in the electronic environment and the impact of such a right on the privacy laws in Malaysia. Secondly, the objective is to examine the possibile application of the relevant provisions of the Personal Data Protection Act 2010 on the right to automatic deletion of data. In order to examine this impact this disucssion will be based upon the European Union data protection laws on the existing right to be forgotten. For instance, what the European Court of Human Rights underlined in *Rotaru v Romania* [4 May 2000, appl. No 28341/95] on data pertaining to the distant past of an individual raises a particular concern as regards to the "private life" protected by Article 8 (1) of the ECHR. Thererfore, this research proposes that a new right to obvilion or automatic data erasers would enable individuals to take control over the use of their own personal data in the Malaysian framework due to the lack of protection under the Personal Data Protection legislation.

Key Words: Privacy; Data Protection; Automatic Deletion of Data

 ISBN 978-967-11350-4-4

INTRODUCTION

The Right to "Oblivion" equally called the right to be forgotten is the right for natural persons to have information about them deleted after a certain period of time. The development of information and communication technologies has been a determining factor as regards to the extending scope of that right. Technological progress has had a considerable impact in this field. The Internet which can be taken as the most representative paradigm of the radical technical and sociological change we are now facing has brought with it a need for a new balance between the free dissemination of information and an individual's self-determination for the dissemination of that information. This balance is precisely what is at stake with the right to be forgotten.

The Internet and its ability to maintain records goes beyond the limits of human memory. Now memory can be one of the rancor, vengeance or belittlement thanks to the "long lasting and eternity effect" of the Internet which preserves memories, good and the bad, errors, writings, photos and videos and the like some of which we would like to remain oblivious at a later stage. Hence, the importance of such a right that proceeds which have information floating around the Web should also have the right to have their data completely removed.

INTERNET PRIVACY

The protection of information of data exchanged during online transactions is the core of Internet security. Violation of this can lead to threatened or damaged or misuse of data of which privacy could be one aspect. When considering "Internet Privacy", "privacy" is not be read as "intimacy" or "secrecy." It rather refers to another dimension of privacy which is the individual's autonomy and the capacity to make choices to keep control over different aspects of one's life. In the context of the Internet this dimension of privacy means informational autonomy or informational self-determination. The Internet handles a vast number of quantities of information relating to individuals. Such personal data are frequently processed; disclosed and disseminated and shared. Some are downloaded and used in all kinds of ways. In this sense the individual's autonomy is in direct relation to personal information Thus the individual should have rights to decide which information about themselves will be disclosed to whom and for what purposes.

THE RIGHT TO BE FORGOTTEN

The first facet of the right to be forgotten is linked to the individual's judicial or criminal past. It was at first mostly related to the creation of criminal records. Today, the right to oblivion of the judicial past has gone widely beyond criminal records. It has been recognised by case law in several countries based on the right to privacy or as part of personality rights. It is justified by the faith in a human being that once he has paid what is due society must offer him the possibility to rehabilitate and restart without bearing the weight of the past errors. However, this right is in conflict with the right of information especially on the Internet and the right to be forgotten.

Firstly, when a decision pronounced by a court or a tribunal is part of judicial news it is then legitimate to refer to this decision mentioning names of those parties to the case. But with time, when it is no more a question of news or current events and as long as there is no longer a justification for re-disclosure of the information as news the right to be forgotten overrides the right to information. There may still be mention of the case, but this should not include parties' names of specific details. Two exceptions can be identified which could override this particular right to be forgotten. For instance, pertaining to facts concerning a matter of historical interest and secondly, for facts linked to the exercise of the public activity by a public figure. In these two instances, the right to information overrides the right to be forgotten.

IMPACT OF ON THE PRIVACY LAWS AND THE PERSONAL DATA PROTECTION ACT 2010

The right of privacy protects a person's right to control the dissemination of information about himself. Research on privacy indicates there to be several dimensions on types of privacy in existence.[1]

Physical privacy (also known as solitude) is the state of privacy in which persons are free from unwanted intrusion or observation.

Informational privacy (also known as anonymity) is the desire to have control over the conditions under which personal data is released.

 ISBN 978-967-11350-4-4

Psychological privacy is defined as the control over released or retention of personal information to guard one's cognitions and affects.

Interactional privacy (also known as intimacy) is relevant to relationships in social units as it preserves meaningful communication between individuals and among group members.

William Prosser organized the subject of invasion of privacy into four areas [2] appropriation, [3] intrusion, [4] embarrassing facts [5] and false light. [6]

The Australian Law Reform Commission, in its Report on Privacy identified privacy as:

(i) The interest in controlling entry to personal territory;

(ii) The interest in freedom from interference with one's person, including "personal space;"

(iii) The interest in controlling one's personal information; and

(iv) The interest in freedom from surveillance and the interception of one's communications.

The objectives of data protections are to protect personal privacy and enable international free flow of personal data by harmonization. The main purpose of the Personal Data Protection Act 2010 is to preserve privacy and enable the enforcement of information processing standards. Two main players involved are the data users and the data protection registrar. Data users are responsible for the personal data. These personal data must be:

1. Obtained fairly and lawfully
2. Used only for registered purposes
3. Disclosed only to registered disclosers
4. Adequate, relevant and not excessive
5. Accurate, and where necessary, up-to date
6. Kept for no longer than necessary
7. Accessible to the data subject
8. Kept appropriately and securely

According to the Data Protection principles the General Principle in section 6 states that the processing (section 4) of personal data requires consent. The Notice and Choice Principle in Section 7 provides that the data users are required to notify the data subjects regarding the purpose for which the data is collected and about the right to request access and correction of the personal data. The disclosure principle in section 8 provides that no personal data shall be disclosed without the consent of the data subject. The Security Principle in section 9 provides that a data user shall take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction. The Retention Principle in section 10 states that the personal data is to be processed for any purpose shall not be kept longer than is necessary for the fulfilment of the purpose to which it was obtained for. The Data Integrity Principle in section 11 provides that a data user shall take reasonable steps to ensure the accuracy and to maintain the data current for the purpose it was collected for.

The Access Principle provides that a data subject shall be given access to his personal data and shall be able to correct the personal data where the data is inaccurate or incomplete. The limitations to the above principles are found in section 3(2) which states that the principles apply only to personal data processed in Malaysia. Section 3(1) Federal and State governments are excluded from complying, whereas credit reporting or referencing agencies will be separately regulated by another law.

ISBN 978-967-11350-4-4

CONCLUSION

As stated above one of the principles of the data protection regime is the purpose principle. This specifies that personal data must be processed for a determined and legitimate and transparent purpose. The right to be forgotten ensues from this principle since, according to one of its applications, the controller of the data may keep personal data in a form which permits identification of subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

This means that personal data may be kept as such if it is justified to achieve the purpose of processing. It should be either anonymised or deleted once the purpose has been achieved or as soon as it is no longer necessary to keep the link with identifiable persons to achieve that purpose. This rule clearly establishes a right to be forgotten. To say the least, the data protection legislation establishes the obligation for anyone who processes personal data to foresee and to respect an expiry date for these data. Hence, with the application of the Personal Data Protection legislation and it its limitations it is doubtful that the right to be forgotten can be overridden from the obligation to delete the data until the purpose is achieved.

REFERENCES

Cho, H. and Larose, R., "Privacy Issues in Internet Surveys" (1999) 17(4) *Soc.Sci Comp. Rev.*, 421-434.

Creech, Kenneth *Electronic Media Law and Regulation* 2nd ed., (Washington: Butterworth, 1996) pg at 301.

This involves the use of a person's name or likeness for commercial gain. For example, an advertisement for Christian Dior using a Jackie Onassis look alike sees: *Onassis* v *Christian Dior- New York* 472 N.Y.S 2d 254 (1984).

The right of privacy also includes the right not to have others intrude on one's solitude or private affairs, if the intrusion would be highly offensive to a reasonable person. Generally cases involving intrusion relate to improper news gathering practices such as illegal surveillance or trespass. For example: a reporter who uses fraud to obtain access to someone's home to take photographs has committed an invasion of privacy. *Douglas* v *Hello! Ltd (No-1)* [2001] EMLR 9; [2001] FSR 732.

At times invasion of privacy action can be brought against the media for the publication of truthful, non-defamatory facts that are embarrassing to an identified individual.

The publication of false or misleading material places a person in a false light in a manner that is highly offensive to a reasonable person with knowledge of, in a reckless disregard as to, or negligence as to its falsity.

Australian Law Reform Commission ("ALRC"), *Privacy* (Report 22, 1983) at *para* 46.