FACTA UNIVERSITATIS
Series: **Law and Politics** Vol. 12, N^{o} 2, 2014, pp. 129 - 135

COMPARATIVE ANALYSIS OF CYBER PRIVACY LAW IN INDIA AND IN THE UNITED STATES OF AMERICA

UDC 342.738:004.738.5](540:73)

Geetika Sood

IEC University at AtalShikshakunj Baddi, Himachal Pradesh, Republic of India

Abstract. *In today's cut-throat competition life, everybody is concerned about one's own privacy. Due to the inculcation of technology in daily life, privacy factor is an increasingly important issue of significant concern for the human being. This paper is an attempt to make a comparative analysis of the cyber law relating to the privacy issue and also to study the applicable law and steps taken by the two countries: one already developed (United States of America) and one of the fastest developing countries (India).*

Key words: *cyber law, privacy, India, United States of America*.

1. INTRODUCTION

Privacy has no definite boundaries and it has different meanings for different people. It is the ability of an individual or a group to keep their lives and personal affairs out of public view or to control the flow of information about them. Privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is to be communicated to others.[1] Privacy is the state of being private and undisturbed, or a person's right to this. It also means freedom from intrusion or public attention, or avoidance of publicity. In fact, right to privacy is more of an implied obligation;[2] it is the right to be let alone.[3]

Submitted August 7th, 2014
Corresponding author: Geetika Sood,
IEC University at AtalShikshakunj Baddi, Plot No. 7 & 10, Atal Nagar, Kallujhanda, Dist. Solan, Baddi, Himachal Pradesh 173205, Republic of India
E-mail: soodgeetika6@gmail.com
[1] Tayal, V., (2011) "Cyber Privacy in the Indian Information Technology Regime: Issues and Challenges" Edn-1st, Bharat Law Publications, Jaipur, p. 17.
[2] Sharma, Vakul (2004), "Information Technology: Law and Practice Cyber Law &E-Commerce", Universal Law Publishing Co. (P) Ltd.
[3] Warren and Brandeis: 'The Right to Privacy" (1890) Harvard Law Review, V IV, p (5).

2. Right to Privacy under Indian Cyber Law

One of the convincing reasons that require safeguarding of privacy rights is the view that personal information is a specific property. Hence, an individual is well within his rights to protect or control any flow of information about him and is legally entitled to protection equal to property ownership protection.[4] Although India has no specific data protection laws, the sphere of personal liberty is regulated by the Constitution of India (Article 21), which has been successfully interpreted in multiple cases dealing with the issue of right to privacy and protection of confidential information.[5] The debate on protecting privacy over the Internet has led to the emergence of many technological and legal changes in this sphere worldwide.

Today, right to privacy is recognized in a number of international documents: the Universal Declaration of Human Rights 1948 (Art. 12); the International Covenant on Civil and Political Rights 1996 (Art. 17); the European Convention on Human Rights (Art.8). The Council of Europe Convention on Human Rights, aimed at securing privacy protection in the context of information technology, came into force in 1985 and, thus far, it has been ratified by 20 states. The Convention laid down the basic principles governing data protection, trans-border flow of information, establishment of consultation committees and procedure for prospective amendment of the EU Convention. The European Union Data Protection Directive 1998 reaffirmed the principles introduced in the EU Convention.

In India, the Information Technology (IT) Act was passed in 2000 in order to deal with the situation in the technological world which has been facing various cyber fallacies. The Act envisages legal provisions on unauthorized access, damage to computer through computer contaminants, hacking, breach of privacy and confidentiality, and publishing false digital signature certificates for fraudulent purposes. Section 66E of the 2000 Information Technology Act includes explicit provisions pertaining to the violation of privacy and defines the terms such as *transmit, capture, private area, publish*, etc.[6]

Further on, Section 72 of the 2000 Information Technology Act prescribes penalty for breach of confidentiality and privacy, directly related to the confidentiality and privacy of individuals.[7] This section is narrow in scope as it is applies only to authorised officials. It means that the provisions envisaged in this section apply only to persons who are authorised to collect data. The application of these provisions is extremely limited under this Act as it covers offences committed only by the authorities such as Adjudicating Officers, members of the Cyber Regulations Appellate Tribunal (CRAT) or Certifying Authorities.[8]

Section 43 of the 2000 Information Technology Act deals with unauthorised access to a computer system and prescribes the penalty and compensation for damage to computer, computer system, etc.[9] Any person who is not authorized to access a computer system is liable under this section if he extracts data and introduces contaminants.

---

[4] Millar, Arthur (1971), The Assault on Privacy: Computer, Data Banks and Dossiers, p. 211.
[5] Case: *Govind v State of Madhya Pradesh*, 1975 2 SCC 148.
[6] The Information Technology (Amendment) Act, 2009, Section 66-E and explanation.
[7] The Information Technology (Amendment) Act, 2009, Section 72 and explanation.
[8] Tayal, Vimlendu (2011), "Cyber Law Cyber Crime Internet and E-Commerce", Bharat Law Publications, Jaipur, p. 210.
[9] The Information Technology (Amendment) Act, 2009, Section 43.

3. New Provisions to PROTECT PRIVACY and Data in India

New provisions on privacy and data protection were introduced in the Indian information technology regime by adopting the Information Technology (Amendment) Act in 2009. Under Section 72A of this Act, any person (including an intermediary) rendering any services under a lawful contract is required to act as stipulated in the terms of contract, and is obliged not to disclose any personal information that could cause wrongful loss or wrongful gain to any person. The breach of this duty is punishable with imprisonment for a term which may extend to three years or with fine up to five *lakh* rupees or both.

At the same time, there are certain limitations and exceptions to one's exercise of right to privacy as set out in Sections 67 and 69 pertaining to a ban against pornographic materials and interest of national security, sovereignty, directions of controller to a subscriber to extend facilities to decrypt information, respectively. With the enforcement of the 2009 Information Technology (Amendment) Act, the amended Section 69 has exemplified Internet censorship which can be justified on sound grounds. This section empowers the Central Government or State Government and its authorised agency to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource if it is necessary or expedient to do so in the interest of the sovereignty or integrity of India, defence of India, security of the state, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence or for investigation of any offence.

Section 69A also allows blocking of certain websites if their content is of such nature as described in Section 69. This provision is in conformity with the reasonable restrictions that are envisaged to be imposed on fundamental rights guaranteed under the Constitution of India, in case the same is found necessary to maintain public order, national integrity, sovereignty and allied interests.

Further, Section 69B empowers the Central Government to authorise any agency of the Government to monitor and collect traffic data or information generated, transmitted or received or stored in any computer resource in order to enhance cyber security and for identification, analysis and prevention of intrusion of computer contaminant.[10]

4. Laws Relating to Privacy in the United States of America (USA)

4.1. Electronic Communication Privacy Act, 1986

The United States of America passed the Electronic Communication Privacy Act (ECPA) in 1986, particularly for the purpose of regulating the Internet-related issues. It is most commonly used for internet privacy lawsuits. This Act prohibits unauthorised intentional access to facility or network and the interception of data. It is also an offence to exceed an authorisation to access a computer facility. The 1986 Electronic Communication Privacy Act (ECPA) provides both criminal and civil penalties for violations of privacy on the Internet. Civil penalties include statutory damages and paying reasonable costs and expenses in individual cases giving rise to class action lawsuits.

[10] Chaubey, R.K. (2009), "An Introduction to Cyber Crime & Cyber Law", Kamal Law House, Calcutta, pp. 45-46.

4.2. Children Online Privacy Protection Act, 1998

The 1998 Children Online Privacy Protection Act (COPPA) was enacted by American Government to protect the privacy of children below the age of thirteen. This Act requires each website operator to obtain verifiable parental consent before collecting, using and disseminating any of the above data. It also provides that the websites aimed at children may not condition a child's participation in a game or receipt of a price on the child's disclosure of personal information.

4.3. Video Privacy Protection Act, 1988

The 1988 Video Privacy Protection Act was enacted to protect the privacy of consumers', rental and purchase of videos. The Act applies to those persons who are engaged in the business of rental, sale or delivery of pre-recorded video cassette tape or similar audio visual materials. It prohibits the disclosure of purchase or viewing history records of individual consumers without their informed written consent in advance of disclosure, with certain exceptions. This statute may create a legal risk for companies streaming videos for fee over the Internet. Disclosure of consumer data could leave these companies open to individual or class action lawsuits. The Act provides for statutory and punitive damages.

4.4. Computer Abuse and Fraud Act, 1984

The 1984 Computer Fraud and Abuse Act (CFAA), often designated as the anti-hacking statute, prohibits unauthorised access to computer systems. The statute provides penalties for unauthorised access and also prohibits exceeding any authorisation. Under the 1984 Computer Abuse and Fraud Act, one may not access a computer with authorisation and use such access to obtain or alter information in the computer. Paragraph 5(A) of this statute also prohibits the transmission of viruses with the intention of causing damage to a protected computer. The violation of this statute implies both criminal and civil penalties. The damages are limited to economic losses and the action must be brought within two years of the violation or within two years of the discovery of the damage. Accordingly, this statute is often featured prominently in internet privacy class action.

4.5. The Health Insurance Portability and Accountability Act, 1996

The 1996 Health Insurance Portability and Accountability Act (HIPAA) includes provisions on privacy rights and confidentiality of health care information in medical records. This Act sets national standards for the protection of privacy of health care information. Thus, any person or entity involved in keeping, transferring and using health information of another is required to ensure reasonable and appropriate administrative, technical and physical safeguards (measures, policies and procedures) in order to:

(a) ensure the integrity and confidentiality of health care information;
(b) safeguard against any reasonably anticipated threats or hazards to the security or integrity of such information as well as the unauthorised uses or disclosure of such information, and
(c) ensure compliance with these safeguards by the officers and employees of such person or entity.

In the United States, apart from the protections provided by the Federal statutes, an individual's private information is also protected by State statutes. A number of States have consumer protection and fraud laws which apply in many cases concerning the violation of privacy and wrongful data-collection practices. For instance, the State of Virginia has included the data collected over the Internet in its Privacy Protection Act. Thus, any company that collects data by means of the Internet may face liability under any or all of these rules in any jurisdiction where the data is available on the Internet.

In nations like India and the United States, right to privacy is not explicitly provided in legal *lexis* but it is accepted as an implied right in the Constitutions of these two counties. In the 1986 Electronic Communication Privacy Act (ECPA), the data holder's consent is given due consideration as the lack of informed consent can be used as a defence in the court of law. From the viewpoint of data protection, the 2009 Information Technology (Amendment) Act of India introduces the distinction between a contravention (infringement) and a criminal offence by introducing the element of *mens rea* for qualifying the criminal offence.[11]

Breach of Online Privacy	
India	USA
a. Under Section 72 of the IT Act, disclosing the personal information without the consent of the person concerned is punishable as a criminal offence involving breach of privacy. Section 66-E also punishes violation of privacy.	a. The Electronic Communications Privacy Act of 1986 is a criminal wiretap statute. On the basis of the recommendation of the Federal Trade Corporation (FTC), the Children's Online Privacy Protection Act (COPPA), effective of 2000, also provides protection to individual privacy. Consent of the individual negates liability.
b. Here, the law is narrow as liability may be imputed only on a person authorised under the IT Act to have access to any electronic book, record, etc. (Section 72 of the IT Act).	b. Section 2511(1)(a) of the ECPA prescribes relevant punishment for any person who commits the breach and/or any person who such liability can be affixed to.

Thus, the United States law has a broader application as it brings within its purview not only the authorised persons but also anyone who intercepts the data. The consent factor is common in the legal provisions of both countries, which is a notable reminder that the informed consent standard has already been recognized and become part of the Organisation for Economic Co-operation and Development (OECD) principles and some other International law instruments. The United States law seems to be exhaustive and extensive as it is particularly a privacy specific legislation. Even after introducing amendments to Section 66E relating to privacy, the Indian provision still does not cover all the areas pertaining to individual privacy. Section 72 is incomprehensive and deficient in more than one way; it is only a brief and isolated legal provision on the right to Internet privacy which regulates the penalty for breach of online confidentiality and privacy.

[11] The Information Technology (Amendment) Act, 2009, amended Section 43 and Section 66.

5. CONCLUSION

Crime is as old as human civilization and cyber crime is as old as the invention of the computer, the wonder machine which changed the lives of human beings. Computers have become an inherent part of everybody's life. They have been put to numerous uses, ranging from personal to professional work and from entertainment to studies. The increasing popularity of computers and their use in each and every field have given rise to other technologies. It will not be wrong to say that computer is the driving force behind the revolution in Information Technology. Due to this, privacy has become a major concern. The Indian 2000 Information Technology Act provides punishment for breach of privacy or confidentiality without the consent of the person concerned under Section 72 of the Information Technology Act, 2000. The violation of privacy is also punishable under the new Section 66-E. In the United States of America, the 1986 Electronic Communications Protection Act (ECPA) is a criminal wiretap statute and the 2000 Online Protection Act also provides protection to individuals' right to privacy. Both countries have been working on this gradually but the privacy factor is an issue of a much greater concern in India than in the United States.

REFERENCES

1. Case: Govind v State of Madhya Pradesh, 1975 2 SCC 148.
2. Chaubey, R.K. (2009), "An Introduction to Cyber Crime & Cyber Law", Kamal Law House, Calcutta
3. Millar, Arthur (1971), The Assault on Privacy: Computer, Data Banks and Dossiers
4. Sharma, Vakul (2004), "Information Technology: Law and Practice Cyber Law &E-Commerce", Universal Law Publishing Co. (P) Ltd.
5. Tayal, Vimlendu, (2011) "Cyber Privacy in the Indian Information Technology Regime: Issues and Challenges" Edn-1st, Bharat Law Publications, Jaipur
6. Tayal, Vimlendu (2011), "Cyber Law Cyber Crime Internet and E-Commerce", Bharat Law Publications, Jaipur
7. The Information Technology (Amendment) Act, 2009, amended Section 43 and Section 66
8. The Information Technology (Amendment) Act, 2009, Section 43
9. The Information Technology (Amendment) Act, 2009, Section 66-E and explanation
10. The Information Technology (Amendment) Act, 2009, Section 72 and explanation
11. Warren and Brandeis: 'The Right to Privacy" (1890) Harvard Law Review, V IV, p. (5).

UPOREDNOPRAVNA ANALIZA ZAKONA O PRIVATNOSTI U KIBERNETSKOM PROSTORU U INDIJI I SJEDINJENIM AMERIČKIM DRŽAVAMA

Usled snažnog prodora i široke primene informacionih tehnologija u svakodnevnom životu, pitanje privatnosti u kibernetskom (cyber) prostoru postaje predmet sve veće zabrinutosti savremenog čoveka. Ovaj rad je pokušaj da se napravi uporednopravna analiza zakona koji se onose na privatnost u kibernetskom prostoru, istraže važeći zakoni i koraci koje su po tom pitanju preduzele Sjedinjene Američke Države kao razvijena zemlja i Indija kao jedna od zemalja koje se odlikuju najbržim stepenom razvoja.

Indijski Zakon o informacionim tehnologijama iz 2000. godine, u članu 72. ovog zakona, predviđa sankcije za povredu privatnosti ili poverljivosti ličnih informacija bez pristanka datog lica. Povreda privatnosti je takođe kažnjiva po novom članu 66 E istog zakona. U Sjedinjenim Američkim Državama, Zakon o zaštiti elektronskih komunikacija iz 1986. inkriminiše prisluškivanje dok Zakon o

zaštiti online komunicacija takođe grantuje zaštitu prava pojedinaca na privatnost. Ove države su postepeno radile na uvođenju zakona iz ove oblasti ali je pravo na privatnost pitanje koje pobuđuje mnogo više zabrinutosti u Indiji nego u Sjedinjenim Američkim Državama.

Ključne reči: *kibernetika, pravo na privatnost, Indija, Sjedinjene Američke Države*.