IMPACT OF EVOLUTION OF CYBER LAW ON HUMAN RIGHTS

Written by ***Ananya Kumar* & Sumedha Ganjoo*****

**Assistant Professor Law, CPJCHS & SOL*

*** Assistant Professor Law, Mewar Law Institute*

ABSTRACT

The Information Technology Act has been passed by the Indian Parliament with an object to facilitate e-commerce, e-governance and to prevent Cyber Crimes. This legislation is unique in many respects. It provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication. It mandates electronic governance and provides infrastructure to achieve that goal. It chalks out an ambitious plan for preventing Cyber Crimes. It provides provision for the appointment of an Adjudicating Officer who shall be an expert in information technology to monitor any contravention and provides for the establishment of Cyber Appellate Tribunal.

It has, however, to be borne in mind that the IT Act is not a separate code for electronic transactions but it is gap filler. It addresses the gray areas spawned by the Internet but does not provide a separate legal regime for electronic commerce. The IT Act has a limited scope. It does not cover all the issues, which have cropped up by the introduction of Internet. While going through various provisions of the IT Act, it appears that many provisions lack harmony and it is quite possible that practical difficulties in applying these provisions will ensure in the near future. The machinery to prevent Cyber Crimes is not well equipped. The Cyber Appellate Tribunal is a one-man Commission, having law degree an essential qualification. Whereas Information Technology involves highly complex technical issues beyond. Internet is an open system of communication with unlimited choices. It has its own culture which is non-hierarchical, open and dynamic. It is in fact anti-thesis of whatever the global society has experienced so far. So, what will be the philosophy of cyberspace law? The primary object of

such a 'philosophy' should be to understand the dynamics of this emerging culture. Also the lawmakers need to address the issue with an open mind without any pre-conceived notions, biases and restrictions.

The question that the emerging cyberspace has thrown in is that- does cyberspace need law? If yes, what should be the parameters? Should the new legislation be just the extension of the old legislation or should it reflect an understanding of the emerging medium? And lastly, what should be the response of the courts in safeguarding citizens, constitutional guarantees vis-a-vis the new medium?

Human rights are given to us by virtue of being born as humans, there is no authority that can abridge those rights. Since these rights are natural rights these can be easily violated by different actors using various techniques and under various pretexts. When we talk of Cyber Space due to its nature, vastness and scope human rights under this space becomes vulnerable and easy to be violated. For instance- a person sitting in U.S can view photos over social networking sites of a person in India without his/her knowledge. This abridges a person's right to privacy.

Some of the human rights concerns in cyberspace are related to Civil and Political Rights such as Free Speech, Defamation, Privacy and Economic Rights like right to enjoy the benefits of scientific, literary, artistic work etc discovery and creation are examined in this research work.

HYPOTHESIS

For the present day life it seems impossible to have a gadget free life. One cannot imagine life without Internet and the use of mobiles and computers is flowing into every generation. The flow of human on internet is tremendous and the unawareness of the harm it can cause is letting the increase of violations of human rights over Internet.

Human rights are given to us by virtue of being born as humans, there is no authority that can abridge those rights. Since these rights are natural rights these can be easily violated by different actors using various techniques and under various pretexts.

When we talk of Cyber Space due to its nature, vastness and scope human rights under this space becomes vulnerable and easy to be violated. For instance- a person sitting in U.S can view photos over social networking sites of a person in India without his/her knowledge. This abridges a person's right to privacy.

Some of the human rights concerns in cyberspace are related to Civil and Political Rights such as Free Speech, Defamation, Privacy and Economic Rights like right to enjoy the benefits of scientific, literary, artistic work etc discovery and creation are examined in this research work.

(a) Freedom of Expression

The Universal Declaration of Human Rights (UDHR), International Covenant on Civil and Political Rights (ICCPR), the European Convention and other international human rights agreements enshrine the rights to freedom of expression and access to information. These core documents explicitly protect freedom of expression "regardless of frontiers," a phrase especially pertinent to the global Internet:

"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media, and regardless of frontiers."

As stated in Article 19, Universal Declaration of Human Rights.

"Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice." As provided under Article 19, International Covenant on Civil and Political Rights. "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of borders." As provided under Article 1o, European Convention for the Protection of Human Rights and Fundamental Freedoms.

No matter what the means, government restrictions on speech or access to speech of others violate basic freedom of expression protections. In addition to direct government censorship of Internet communications, or privatized censorship, freedom of speech in the Internet is threatened by diverse factors.

Blocking, filtering, and labelling techniques can restrict freedom of expression and limit access to information. Government-mandated use of blocking, filtering, and label systems violates basic international human rights protections. Global rating or labelling systems squelch (crush down) the free flow of information. Efforts to force all Internet speech to be labelled or rated according to a single classification system distort the fundamental cultural diversity of the Internet and will lead to domination of one set of political or moral viewpoints. Diversity and user choice are essential: To the extent that individuals choose to employ filtering tools, it is vital that they have access to a wide variety of such tools[1].

"Self-regulatory" controls over Internet content, which have been promoted by some as an alternative to government regulation, ought not to place private ISPs in the role of police officers for the Internet. With regards to content, what is being suggested in the name of "self-regulation" is not that ISPs should as a group regulates their own behavior, but rather that they should regulate the speech of their customers. This is not true "self-regulation." The role of an Internet Service Provider is crucial for access to the Internet and because of the crucial role that they play. ISPs have been targeted by law enforcement agencies in many countries to act as content censors. While ISPs ought to provide law enforcement reasonable assistance in investigating criminal activity, confusing the role of private companies and police authorities risks substantial violation of individual civil liberties[2].

Human rights discourse in the IPR regime has added a new approach to that analysis of the content and scope of IPR's[3]. As an embodiment of expressional act, IPR has important

[1] A Starting Point: Legal implications of Internet Filtering, A Publication of the OpenNet Initiative, available at ,http://www.opennetinitiative.org , visited 12 Feb 2017.

[2] Sunstein R, Cass, The First Amendment in Cyberspace, The Yale Law Journal, Vol.104, N0.7, May 1995, available at http://www.jstor.org/ , visited on 9 Jun 2017

[3] Bhat P, Ishwara, Historical Evolution and Development of IPR,1 KLJ [2017] at p, 6 (Kare Law Journal, Issue 1, November, 2017)

human rights dimension. Internet assists in the promotion of learning and research and at the same time it might impact upon the rights of copyright holders. Copyright law's basic inclination to support liberty and is an expressional freedom rather than a tool of censorship. Internationalization of intellectual property law with the same purpose, rather than treating it as sheer object of trade is contemplated in human rights philosophy.

Jurisdiction – It is not enough for the State to recognize the basic human rights but it should also provide appropriate mechanism for enforcing them through competent courts. To determine the jurisdiction of the courts is very difficult owing to the multi-jurisdictionality nature of the Internet[4]. Determination of jurisdiction for the enforcement of rights cyberspace entities is vital but needs different treatment in this new environment.

Keeping the above in mind the Hypothesis for the research work is formulated as follows; " Legal and Regulatory model for the protection , promotion and enforcement of human rights of cyberspace entities is possible only with the co-operation of sovereign nation-states, who should collaborate, and act together to decide on appropriate best practices, models and legislation to handle human right issues in cyberspace; and to strengthen the international legal system and establish international institutions to meet the challenges posed by new information and communication technologies for the national and international legal regimes"

Following Research Questions have been raised in order to test the Hypothesis;

(a) Freedom of Speech and Expression: - Should the Online world continue to be a freewheeling, unregulated "market place of ideas" or things have gone out of control? If restrictions are appropriate, what steps should be taken? What is the standard of obscenity or indecency?

(b) Anonymity & Harassment: - What is the nature of threats posed by online flamers, cyber stalkers and online harassers? What steps might be taken to keep cyberspace safe and to prevent hate and hatreds?

[4] See generally Yahoo! Inc V LA LIGUE CONTRE LE RACISME ET L'ANTISEMITISME, A French Association, No.01-17424, D.CNo.cV-00-21275-JF, decided by northern District Court of California;

(c) Privacy: - Why are electronic privacy rights so much weaker than analogous rights in other venues? Does the public care? Should the public care? How judiciary has responded to the threat of privacy?

(d) Shreya Singhal v. UOI

(e) Aadhar affect on cyber security

And even if these questions are resolved, how can such laws are enforced? How human rights of cyberspace entities can be enforced?

Methodology Doctrinal method has been employed to do the research work. Research involves analysis of case law, arranging, ordering and systematizing legal propositions and study of adjudicatory decisions of legal institutions. Authoritative books on cyber law, national legislations, statutes of states, Government reports and international treaties were part of the primary source of research and internet, journals, articles, periodicals, Private Institutions reports were used as secondary sources of research. A critical and analytical method was employed in the analysis of the RIGHTS of the entities involved keeping in view of the judicial decisions of US, European countries and Indian courts. Internet was invented by the US Government initiative and US courts had the first opportunity to examine and determine the legal issues raised by internet technology. Hence most of the research work uses US court decisions and legislations for the purpose of analysis.

FREEDOM OF EXPRESSION IN CYBERSPACE

"Any *content-based regulation of the Internet, no matter how benign the purpose, could burn the global village to roast the pig".*

-Stewart Dalzell, J.

With the advent of Internet, there has been a subtle shift in the law making as well, *i.e.*, law is now no longer meant for the man only, it is now for the machines as well. For example, law has been able to recognize the computer as tool in criminal activity.

A computer could now be referred to as a 'weapon of offence' as well as a 'victim of crime'. What is being witnessed is - emergence of cyberspace jurisprudence.

CYBERSPACE: TO LEGISLATE OR NOT

Internet is an open system of communication with unlimited choices. It has its own culture, which is non-hierarchical, open and dynamic. It is in fact anti-thesis of whatever the global society has experienced so far. So, what would be the 'philosophy of cyberspace law'? The primary objective of such a 'philosophy' should be to understand the dynamics of this emerging culture. Also, the lawmakers need to address the issues with an open mind without any pre-conceived notions, biases and restrictions.

The question that the emerging cyberspace has thrown in is that - does cyberspace need law? If yes, what should be its parameters? Should the 'new' legislation be just an extension of the 'old' legislation or should it reflect an understanding of the emerging medium? And lastly, what should be the response of the courts in safeguarding citizens' constitutional guarantees vis-a-vis the new medium?

For the purpose of clarity, a *Table* has been provided to summarize the judgments given by the different courts in the matters related to CDA and COPA.

Case	**Court**	**Legislation in Question**	**Verdict**
American Civil Liberties Union, (ACLU) v. *Janet*	The District Court for the Eastern District of	Communications Decency Act, 1996 (CDA).	The CDA [47 U.S.C. § 223] is unconstitutional

Reno, Attorney-General of the United States (Reno I)	Pennsylvania.		and that the First Amendment denies Congress the power to regulate protected speech on the Internet.
Reno v. *ACLU, (Reno II).*	US Supreme Court	Communications Decency Act, 1996 (CDA).	The CDA suppresses a large amount of speech that adults have a constitutional right to send or receive. It is patently invalid and unconstitutional
ACLlL.v. Reno, (Reno III)	District Court for the Eastern District of Pennsylvania.	The Child Online Protection Act, 1998 (COPA).	The COPA imposes a burden on speech that is protected for adults. The court preliminarily enjoined enforcement of COPA.
ACLU v. *Reno, (Reno IV)*	US Court of Appeals for the Third Circuit	The Child Online Protection Act, 1998 (COPA).	COPA's use of " contemporary community standards" to identify material that is harmful to minors rendered the statute substantially overbroad.
Ashcroft, Attorney General v. *American Civil Liberties Union, et al*	US Supreme Court	The Child Online Protection Act, 1998 (COPA).	COPA's reliance on community standards to identify "material that is harmful to minors" does not *by itself* render the statute substantially overbroad for

			purposes of the First Amendment. The Government was enjoined from enforcing COPA.

FREEDOM OF EXPRESSION AND THE INDIAN CONSTITUTION

The Indian Constitution lays down under Article 19 certain fundamental rights to every citizen. The Art. 19 uses the expression 'freedom' and mentions the several forms and aspects of it, which are secured to individuals, together with the limitations **that could** be, **placed** upon them in the general interest of the society.

Reasonable Restrictions

Article 19(l)(a) provides "that all the citizens shall have the right to freedom of speech and expression". But it should be read with sub-Art. (2), which imposes reasonable restrictions imposed by the State relating to (i) defamation; (ii) contempt of court; (iii) decency or morality; (iv) security of the State; (v) friendly relations with foreign states; (vi) incitement to an offence; (vii) public order; (viii) maintenance of the sovereignty and integrity of India.

Hence a law made in respect of the matters referred to in Art. 19(2) must prima facie be presumed to be constitutionally valid and due weight must be given to the legislative judgment on the question of reasonableness, though that judgment is subject to judicial review.

According to Seervai, H.M.,[5] it is difficult, if not impossible, to read into the words "reasonable restrictions" the test of "clear and present danger"[6] evolved by the US Supreme Court in dealing with the freedom of speech and the press. The difference between the First Amendment of the US Constitution and Art. 19(l)(a) was noted by Douglas J. in *Kingsley Corporation* v.

[5] Seervai, H.M., Constitutional Law of India : A Critical Commentary, Vol. I (1975), N.M. Tripathi, Bombay.
[6] It is important to note that the test of "clear and present danger" has been rejected by the Supreme Court in *Babulal Parate* v. *Maliarashtra,* AIR 1961 SC 884: (1961) 3 SCR 423: (1961) 2 Cr LJ 16.

Regents of the University of New York,[7] in holding that all pre-censorship of cinema films was constitutionally void, he said:

> "If we had a provision in our constitution for 'reasonable' regulation of the press such as India has included in hers there would be room for argument that censorship in the interest of morality would be permissible".

In other words, the Indian Constitution provides that even freedom of speech must yield to public order, *i.e.* "liberty with order". It was held by the Supreme Court in *MM. Devendrappa* v. *Karnataka State Small Industries Development Corpn.*[8]

"The fundamental freedoms enumerated under Art. 19 are not necessarily **and** in all circumstances mutually supportive, although taken together they weave a fabric of free and equal democratic society, e.g., the right to reside and settle in any part of the country can be put in jeopardy by a vociferous local group freely expressing its view against persons from another part of the country. Freedom of speech of one, affects the freedom of movement of another…..

Some restriction on one's rights may be necessary to protect another's rights in a given situation. The rights must be harmoniously construed so that they are properly promoted with the minimum of such implied and necessary restrictions".

FREEDOM OF EXPRESSION AND THE INTERNET

Keeping in view the concept of "liberty with order", application of the freedom of expression in the context of Internet would be a restrictive one. The courts would have to first understand the nature of the Internet medium before selectively applying the reasonable restrictions as set out in Article 19(2).

[7] (1959) 360 US 684: (1959) 3 L Ed 2d 1522.

[8] (1998) 3 SCC 732: AIR 1998 SC 1064: 1998 AIR SCW 850.

As it was held in *K. Narayanan* v. *State*[9] that "the freedom of speech and expression guaranteed by Article 19(l)(a) included the freedom to acquire knowledge, to read books and periodicals and read any type of literature, subject only to reasonable restrictions being placed on such rights" .

Thus fundamental right to freedom of speech and expression extends to the Internet medium as well. Every citizen has a freedom to acquire or share knowledge (or information) using Internet and related resources, subject only to reasonable restrictions. In fact, the courts may apply reasonable restrictions in the interest of decency or morality to restrict the publication of information which is obscene in electronic form. For this purpose the courts may have to invoke reasonable restrictions in the interest of decency or morality in light of sections 67, 67A and 67B of the Information Technology Act, 2ooo which deals with publication or transmission of obscene material in electronic form.

Earlier as per the Gazette Notification (Extraordinary) No. G.S.R. 181(E), dated 27th February, 2oo3, Indian Computer Emergency Response Team (CERT-In) had been designated as the single authority for issuing of instructions in the context of blocking of websites, as there is no explicit provision in the Information Technology Act for blocking of websites. The aforesaid notification was based on the premise that such blocking can be challanged if it amounts to restriction of freedom of speech and expression. However, the websites promoting hate content, slander, or defamation of others, promoting gambling, promoting racism, violence and terrorism and other such material, in addition to promoting pornography, including child pornography, and violent sex can reasonably be blocked since all such websites may not claim constitutional right of free speech. Blocking of such websites may be equated to "balanced flow of information" and not censorship.

The question is how far the concept of "balanced flow of information" could be streched. For example, earlier CERT-In attempted to block Meghalaya secessionists email group (groups.yahoo.com/gro-ups/kynhun) and it led to blocking of the entire Yahoo Groups site

[9] (1998) 3 SCC 732: AIR 1998 SC 1064: 1998 AIR SCW 850.

by the overzealous ISPs, with the result complete blackout of communication among the other legitimate users of the Yahoo Groups.

Interestingly, the Central Government has rescinded the aforesaid notification *vide* Gazette Notification G.S.R. 41o(E) dated 17th May, 2o1o. In other words, CERT-In is no longer empowered to block websites or content. The District Court of Delhi in *Lacoste SA.* v. *Ninety Nine Labels (P) Ltd.,*[10] *Tommy Hilfiger Licencing LLC* v. *Ninety Nine Labels (P) Ltd.,*[11] and *Polo Lauren Company* v. *Ninety Nine Labels (P) Ltd.,*[12] has opined[13] that the Gazette Notification (Extraordinary) No. G.S.R. 181(E), dated 27th February, 2oo3 has been rescinded *vide* Gazette Notification G.S.R. 41o(E) dated 17th May 2o1o, hence CERT-In is neither a proper or necessary party to block websites or contents thereof. This raises an interesting question - what would be the remedy, if someone is aggrieved by defamatory or obscene content?

DATA SECURITY AND DATA PROTECTION

In the present scenario citizens avail of a variety of services from government and private organisations. These transactions involve the furnishing of large amounts of data that is usually comprised of sensitive or personal information. This information is often required for the provision of the service sought to be availed, however, there may be cases wherein such data is collected for collateral purposes. Further, security of data collected for legitimate purposes from intrusive attacks by criminal elements is a large concern.

Therefore, the Information Technology (Amendment) Act, 2oo8 introduced Section 43-A with the purport of creating privacy protection for information held by private intermediaries. It seeks to prevent unauthorised disclosure of "sensitive personal data or information".

> 43-A. *Compensation for failure to protect data.*—Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a

[10] TM No. 310/2013.
[11] TM No. 311/2013
[12] TM No. 312/2013
[13] Vide order dated 23.7.2914

> computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

The section applies to "body corporates". Body corporates are defined in the explanation appended to the section by including any company including a firm, sole proprietorship or an association of persons. The definition of body corporates herein is expanded to include sole proprietorship that has been otherwise precluded from such classification. Government departments have been excluded from the definition of body corporates. Therefore, this provision does not cast any obligations on government agencies.

Another key determinant of the limited data security envisaged under this provision is "reasonable security practices and procedures". This is defined under the second explanation appended to the provision which states:

43-A. *Compensation for failure to protect data.—...*

> (ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

PERSONAL INFORMATION DEFINED

There is no definition available in the main statute for sensitive personal data or information or personal information. However, a key determining factor to establish due diligence requirements is the holding of sensitive personal data under Section 43-A. The third explanation appended to the section provides for the Central Government to define the same in

consultation with professional bodies. Pursuant to this the government enacted the Information Technology Act. (Reasonable Security Practices and Procedures^and Sensitive Personal Data or Inform ation) Rules, 2011 hereinafter referred to as Personal Data Rules.

DATA PROTECTION IN INDIA

Section 43-A does not specifically define the nature and extent of security practices. The Central Government is empowered to establish such standards arguably to maintain dynamism of the law with respect to changing technology. The Personal Data Rules were formulated to establish such standards and practices and at present is the most comprehensive form of data protection prescribing protocols and procedures for bodies corporate.

The Personal Data Rules ascribe a specific obligation upon private bodies dealing in personal or other information to formulate a privacy and disclosure policy. Rule 4 of the Personal Data Rules:

> 4. *Body corporate to provide policy for privacy and disclosure of information.*—
> {1} The body corporate or any person who on behalf of body corporate collects, r eceives, possess, stores, deals or handle information of provider of information, sha ll provide a privacy policy for handling of or dealing in personal information inclu ding sensitive personal data or information and ensure that the same are available f or view by such providers of information who has provided such information under lawful contract. Such policy shall be published on website of body corporate or an y person on its behalf and shall provide for-

DISCLOSURE OF INFORMATION

The real threat to privacy lies in the unlawful disclosure of personal or private information. Therefore, any data protection ought to offer a mechanism to regulate information collected. Rule 6 enunciates the circumstances in which disclosure may be made:

> 6. *Disclosure of information.* — (1) Disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information, who has provided such information under lawful, contract or otherwise, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation:
>
> Provided that the information shall be shared, without obtaining prior consent from provider of information, with Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences. The Government agency shall send a request in writing to the body corporate possessing the sensitive personal data or information stating clearly the purpose of seeking such information. The Government agency shall also state that the information so obtained shall not be published or shared with any other person.
>
> (2) Notwithstanding anything contained in sub-rule (1), any sensitive personal data on information shall be disclosed to any third party by an order under the law for the time being in force.
>
> {3) The body corporate or any person on its behalf shall not publish the sensitive personal data or information.
>
> (4) The third party receiving the sensitive personal data or information from body corporate or any person on its behalf under sub-rule (1) shall not disclose it further.

The Rule incorporates the concept of consensual disclosure to third parties. Consent would have to be obtained to lawfully affect disclosure in case the contract under which the information was provided is silent on the issue. Otherwise, the contractual term governing disclosure shall be applicable.

Sub-rule (2) further prohibits public disclosure or publishing of sensitive personal data or information. Further, sub-rule (3) casts an obligation upon the third party to maintain the integrity of the consent accorded by the provider by not disclosing such information further.

This provision is prone to misuse since in certain cases the provider of information is not the individual concerned with the personal data. Rule 6(3) specifically prohibits the body corporates from publishing any sensitive personal data or information.

The transfer of sensitive personal data to anybody, organisation, or country is permitted only if *it* is ensured that same level of data protection would be accorded. The transfer can only take place for the performance of a lawful contract or where the transfer has been consented to.[14] Rule 7 lays down that information will be shares with government agencies mandated under law without obtaining prior consent for the purposes of verification of identity, for prevention, detection, investigation including cyber incidents, prosecution, and punishments of offences. This provision is in conflict with the aforesaid provision on consent and non-disclosure. Further, it is desirable that a procedure may be laid down in this regard in a manner akin to the exercise undertaken by the Supreme Court in *People's Union of Civil Liberties* v. *Union of India*[15]. **It** is amply clear that privacy as a right is derived from Article 21. Article 21 mandates that the right protected by it may only be abridged by a procedure established by law. On that count this provision prima facie fails to meet that standard.

DATA SECURITY

Safety of protected data is a significant concern for data protection laws. This is largely to prevent breach and misuse of information. It further prevents crimes such as online fraud, identity theft and financial crimes among others.

[14] R.7, Information Technology (Reasonable Security Practices and Procedures and Sensitive personal Data or Information Rules, 2011.
[15] (1997) 1 SCC 301: AIR 1997 SC 568.

(1) Reasonable Security Practices and Procedures.(1) A body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies.

(2) The international Standard IS/ISo/IEC 27oo1 on "Information Technology—Security Techniques Information Security Management System—Requirements" is one such standard referred to in sub-rule (1).

(3) Any industry association or an entity formed by such an association, whose members are self-regulating by following other than IS/ISo/IEC codes of best practices for data protection as per sub-rule (1), shall get its codes of best practices duly approved and notified by the Central Government for effective implementation.

(4) The body corporate or a person on its behalf who have implemented either IS/ISo/IEC 27oo1 standard or the codes of best practices for data protection as approved and notified under sub-rule (3) shall be deemed to have complied with reasonable security practices and procedures provided that such standard or the codes of best practices have been certified or audited on a regular basis by entities through independent auditor, duly approved by the Central Government. The audit of reasonable security practices and procedures shall be carried out by an auditor at least once a year or as and when the body corporate or a person on its behalf undertake significant up gradation of its process and computer resource.

Rule 8(1) lays down that there must have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational, and physical security control measures. In the event of a breach, the body corporate must be able to demonstrate that they have implemented security control measures.

This includes being IS/ISo/IEC 27oo1 compliant. on any annual basis the body corporate must undergo an audit of his/her reasonable security practices.[16]

The Rules discussed hereinabove provide a beginning to the cause of a data protection in India. However, it contains large scope for misuse. For instance, the use of the term providers of information instead of individuals concerned allows body corporates to accord rights effectively due to the individuals to whom the information pertains. Therefore, the requirement for a comprehensive law on data protection that encompasses government and private agencies remains unfulfilled.

The province of privacy that is protected under technology laws refers largely to the online space in terms of communication privacy and information privacy, *i.e.* data protection. The framework provides for procedural and substantive safeguards that govern the collection and retention of the data. It further, defines the security standards to protect individuals from data theft and other online crimes. This regime is based on principles of privacy protection although some provisions fall short of the same.

The dynamic nature of technology and its use across the board gives rise to a new facet of privacy protection. The aforesaid legal position in some measure provides protection in this regard. However, the legal framework is not in tune with contemporaneous realities that hamper the implementation of the law. The internet specifically is not exclusively amenable to the powers of the State; it is largely controlled by the private sector along with other stakeholders. Therefore, the protection of privacy should be modelled on co-regulatory format that enhances compliance whilst reserving certain limited circumstances that would give rise to intervention of State agencies.

The conception of privacy under the Information Technology Act, 2ooo is fairly limited in view of the position taken in jurisprudence across jurisdictions. It does not fully comprehend the extent to which the ordinary citizen's right to life is exercised online. Therefore, the protection regime lacks robustness.

[16] R. 8(4), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

THE AADHAAR CARD PROJECT

The National Identification Authority Bill, 2o1o is a proposed legislation to provide a statutory basis for the National Identification Project with the objective of issuing unique identification/aadhaar numbers that is based on biometrics to residents on voluntary basis. The following personal information will be collected for issuance of an Aadhaar number—Name, Date of Birth, Gender, Fathers/Spouse/Guardian's name, Mother/Spouse/Guardians name and Address; Photograph, all 1o fingerprints and both iris scan. In addition, information about bank account, introducer, consent, mobile number, email address and the document on which the enrolment is based may be collected.

The Bill provides for the establishment of a National Identification Authority of India (NIAI) for the purpose of implementation of the proposed Act. Further, it laid down the manner of authentication of such individuals, establishment and composition of Authority, functions of Chairperson, and protection of information relating to an Aadhaar number, and penalties for impersonation, unauthorised access, and the power to make rules and regulations in this regard. The NIAI Bill contains detailed provisions on several aspects of the unique identification number and its administration.

Various government services such as subsidies have unique identification numbers as a mandatory prerequisite. Therefore, the voluntary nature of collection of information under the aforesaid legislation is vulnerable. For instance under Section Z3(z)(&) of the proposed Act states:

> *(k)* sharing, in such manner as may be specified by regulations, the information of aadhaar number holders, with their written consent, with such agencies engaged in delivery of public benefits and public services as the Authority may by order direct.

It lays down the position that written consent would be obtained for disclosure of information to third parties for the purpose of delivery of public benefits and services. There is no provision in the law that protects any individual who refused to grant such consent. In other words, services would be denied to an individual who refuses to provide their number. There is another concern that many of the number holders may be illiterate, it may not be reasonable for them to accord consent upon effective understanding of the implications thereof.

Therefore, in effect the voluntary nature of the collection of information is compromised.[17] There is precedence to suggest that in cases wherein there is mandatory collection of information the same may be anonymised upon the lapse of stipulated time period. This is of vital importance when the personal information collected may become part of a public database.

Hence, it is important to consider that the present legislation is before Parliament in the absence of any law regarding data protection or privacy. A similar concern has been raised in the Standing Committee Report on the legislation. Further, the aforesaid report records expert evidence the effect that there is a large risk of unlawful intrusion and disclosure of private information collected under the proposed legislation. The Report records the government's intention to enact a statute with respect to data protection and privacy in such matters along with institutional safeguards within the framework envisaged in the proposed legislation.[18]

The mandatory collection of personal information also creates concerns of infringement of the right guaranteed under Article 2o(3). Denying services, and rights, to persons because they are unwilling to part with the information under the proposed legislation poses a great risk to the rights of the innocent and offenders alike. In similar circumstances the Supreme Court of Philippines has held: "The data may be gathered for gainful and useful government purposes; but the existence of this vast reservoir of personal information constitutes a covert invitation to misuse, a temptation that may be too great for some of our authorities to resist".[19]

The Supreme Court by virtue of a number of decisions has laid down the procedure by which the right to privacy may be abridged in certain paramount interests such as national security, law and order, etc. The Supreme Court laid down the procedure specifically with respect to the power of interception of phone calls by the government under Section 5(2),

[17] Report of the Group of Experts on Privacy, chaired by A.P. Shah J. Report 48.
[18] Ibid, Report 11.
[19] Puno J (1998), Ople v. Torres, GR No. 127685, dt. 23.07.1998 (Supreme Court of Philippines).

Telegraph Act, 1885.[20] It is trite law that the procedure ought to be in consonance with the due process standard, as explained in the *Maneka Gandhi* v. *Union of India*[21].

The settled law in this respect has not been followed in respect of the disclosure of personal information under the proposed legislation. This is demonstrated by a provision *pari materia* to Section 5(2), Telegraph Act, *i.e.* Section 33(6) of the Bill which states:

> any disclosure of information (including identity information) made in the interests of national security in pursuance of a direction to that effect issued by an officer or officers not below the rank of Joint Secretary or equivalent in the Central Government specifically authorised in this behalf by an order of the Central Government.

There is no provision in the framework envisaged for effective notice being provided for breach or change in privacy policy. In order ensure transparency the authority ought to be mandated by law to demonstrate to number holders that all steps are being taken in compliance with privacy principles. Further, Section 23 of the proposed Act provides wide powers to the authority for sharing of information pursuant to memoranda of understanding entered into with the Central Government, State Government or any other agency, the same is prone to misuse and the threat of unlawful disclosure. Therefore, the chance of tampering and unlawful disclosure is accentuated and inadequately protected by the various penal provisions in the bill.

Further, the proposed Act lays down that the authority will reply to an authentication request with a yes or no answer, or with any other appropriate response. This introduces the possibility of another response, and may negate the privacy protection of only a yes or no answer, by introducing the possibility for another response.[22]

It is clear that the proposed legislation has grave implications for the rights of individuals to privacy and data protection particularly in the absence of any law to that effect. The need of

[20] People's Union of Civil Liberties v. Union of India, (1997) 1 SSC 301: AIR 1997 SC 568.
[21] (1978) 1 SCC 248: AIR 1978 SC 597.
[22] S.5, National Identification Authority Bill, 2010.

the hour, therefore, is a clear law protecting rights in this regard and defining the limitations of such rights.

Shreya Singhal V. UOI: Resurgence Of Freedom of Speech And Expression In The Internet Age.

The Supreme Court on the 24.o3.2o15 has rightly struck down the most draconian provision of the Information Technology Act, 2ooo, preceding a couple of incidents which shocked the conscience of the entire nation. The ardent effort of the Government to save the said provision "66A of the IT Act, 2ooo" by administering it in a reasonable manner was rightly rejected by the Supreme Court judging the provision on its sole merits. The Supreme Court fundamentally rejected this feign argument because Governments may come and Governments may go, but the provision "66A" shall go on forever thereby not binding the successor Government subjecting it to misuse and resulting in a never ending dilemma. This article examines the provision in the light of what is being hash tagged as landmark #SocialMediaVerdict. The Section 66A of the Information Technology Act, 2ooo, which came into effect by the Amendment Act of 2oo9, is produced hereunder:

66A. Punishment for sending offensive messages through communication service, etc.

Any person who sends, by means of a computer resource or a communication device,—

(a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device,

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation.— For the purpose of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, images, audio, video and any other electronic record, which may be transmitted with the message.

Well, colonialism leaving a much longer impact than thought, the genesis of this Section can be traced back to Section 1o(2)(a) of the U.K. Post office(Amendment) Act, 1935, which made it an offence to send any message by telephone which is grossly offensive or of an indecent, obscene, or menacing character; which was later reproduced in Section by Section 66 of the UK Post office Act, 1953. Thereafter, the section was amended a couple of times and in its present form in the UK, it is Section 127 of the Telecommunication Act, 2oo3; wherein it condemns the improper use of public electronic telecommunications network. The Supreme Court has further very categorically discussed the scope of Section 66A of the IT Act under various broad heads. This article, further endeavours to briefly explain each of them below:

CONCLUSION

Proposed Frame work:

To observe privacy In Indian work culture we have to adopt above framework which clearly define general guidelines of information addressing in different phases. In this we cover all the necessarily measures while considering the threat to privacy and try to remove vulnerability present in the system. This model mitigates the risk to privacy to the appetite level. So that further threaten to privacy will reduce its impact. We divide the privacy protection in four phases Data Collection, Data Security, Data Process, and Data Access which describe are as follows.

(a) Data Collection:-

First step of privacy protection is start with data collection itself, there must be strict data collection policy impose by the top authority which clearly mentions the following points:

- Information is collected by authorize appointed agency only.
- Information is collected for lawful purpose only.
- Personal data shall be adequate, relevant and not excessive.
- Purpose of information collection must be mention.

If we capture the information properly then it is easy to maintain the information security in next steps. Government shall authorize the agencies for data collection government must also insure that they follow the regulation by doing periodic audit. Whenever information needs for collection it must be collected for lawful purpose only its commercial use is strictly avoided

(b) Data Security and Storage

After data capture, personal data shall be kept accurately and kept up-to-date. Appropriate technical and organizational measure shall be applied. Technical measures include all information security controls which are necessary to keep information security over internet. If data is store on the server then that server must be fully controlled by government of India. Server must be taken all security safeguard against unauthorized access, use and other modification. organization measure includes classification of information according to its nature. 'Segregation of Duties' and 'Need to know' arranges the information according to its need no single person have full control over information user subject is fully mapped with its all information components.

(c) Data Process

Personal data shall be process fairly and lawfully here processing means not only computer processing. We have to process data only when the consent of user is involved, if the user is in contract and one of the party of the contract, process if it's required for judicial proceeding, process if its legitimate use for national interest, process if it's vital interest of data subject. Data should be process for only given purpose. After processing, the data must be properly disposed. Retention policy must be specified as including purpose and duration of retention.

(d) Data Access

The data access must follow Need to Know Basis. There must be control that information not goes beyond the Indian Territory. If data is going beyond territory then appropriate control must be taken to ensure that information is protected outside the India, there must be legal obligation between two countries about data handling. Within the country any Indian or non government industry process the data they must have to follows all above the norms followed by the Indian government.

Findings

(a) e-Governance

There is unique privacy challenges associated with e-governance due to large storage of personal and sensitive data. obviously e-governance has given new dimension to development and globalization but there should be systematic improvements in governmental privacy leadership; and other technology-specific policy rules limiting, how the government collects and uses personally identifiable information. Government also has unparalleled opportunity to lead by example, by establishing strong, consistent rules that protect citizens without harming the government's ability of functioning. To achieve the specified goal we have to follow certain guidelines like:

- Creating a Union Chief Privacy officer
- Installing chief privacy officers (CPos) at all major departments
- Ensuring that Data Mining techniques are addressed by the Privacy Act
- Strengthening and standardizing privacy notices including "privacy impact assessments"
- Privacy Protection on agency website
- Complaint processing in case of breach of privacy

(b) e-Jurisdiction

Finally India got its first awaited model e-Court at the Ahmedabad City. Evidently the implementation of ecourt in India is in its commencing state .The issues like privacy are still untouched. Without substantiation of the standard of technological framework and processes

used by e-courts, the system of certainty upon which the courts and law are based has the potential to become inherently uncertain. It will be better to embed the privacy frame work to e court instead of including it later. The e-court must provide security and privacy of electronic filings. Court shall make any document that is filed electronically publicly available online."

- There must be unified and coherent policy for the privacy protection and access rights.
- Except where otherwise noted, the policies apply to both paper and electronic files.
- The availability of case files at the courthouse will not be affected or limited by these policies.

(c) e-Media

e-Media include television channels, radio, internet podcast, and all electronic journalism which are used by today's media. Main purpose of media is to bridge the gap between government policy and public grievances. As there is no information classification in India every information is floated over the media its adverse impact is seen at 26/11 incident all government moves are shown on TV channel which is used by terrorist as a feedback they make their attack strong. Privacy is most concern about celebrities but media is big threat to their privacy every gossip of celebrity is become a Breaking new in most of the new channel. Casting couch is very popular tool used by media now a day which directly hammer the individual privacy. There is no guideline to handle this issue privacy frame will provide solution to solve this problem.

(d) BPO

BPO is Business process outsourcing in IT/ITES industries. BPO play major role for revenue generation in India, complement to BPO there are other types of industries also well establish like KPO (Knowledge process outsourcing), LPO (Legal process outsourcing) and others this is majorly based on information processing. India's BPO industry grew 6o percent to US $6.6 billion in the fiscal year ending 31 March 2oo8, according to the National Association of Software and Service Companies (NASSCOM), in New Delhi. India's business process outsourcing, or BPo, industry says its security standards match the best in the world. There has never been a major instance of data theft in India. Nonetheless, companies in the United States do fear such an event, says Richard M. Rossow director of operations at the U.S.-India Business

Council in Washington, D.C. The fear is "not because they are at a higher risk of such a thing taking place in India, but rather because public perception of sending work to India is so bad that it will take only one major event for the affected company to 'pull the plug' on their India data service venture."

If we do not ensure companies about strong privacy protection framework, we will lose outsourcing sector. We still rely on some international standard but unless if we not have legal framework, it will difficult to safeguard stake holder interest. Privacy at work place is also ignored field, thousands of workers are work in the premises as ‘people are the weakest link in information security’ there must be guideline at work place like cell phone are strictly avoided, prior screening of employee, all work under electronic surveillance, technology used to access employees computer.

(e)Telecommunication:

Service providers (SPs) including Internet service providers, number-database operators, telecommunications contractors, emergency call persons; public number directory publishers, authorized researchers and their respective employees must protect the confidentiality of information. The use or disclosure of any information or document which comes into their possession in the course of business must be restricted .This could apply, for example, to law enforcement officers who receive billing information, who may receive information in connection with their functions, publishers who receive information in connection with the publication and maintenance of a public number directory, or other service providers who may have received information for billing or network maintenance purposes.

(f) Health

Health sector is the important concern in privacy. Your health information includes any information collected about your health or disability, and any information collected in relation to a health service you have received. Many people consider their health information to be highly sensitive. Before proceeding it is very important to consider what all the issues that come under Health Information are:

- notes of your symptoms or diagnosis and the treatment given to you

- your specialist reports and test results
- your appointment and billing details
- your prescriptions and other pharmaceutical purchases
- your dental records
- your genetic information
- Any other information about your race, sexuality or religion, when collected by a health service provider.

There is certain legislative framework also prepared in other countries for the privacy issue like HIPPA and PSQIA Patient Safety Rule made by US government. Keeping all this in mind it is mandatory to have a proposed system of health domain that mainly focused on privacy from Indian perspective. We must have administrative safeguard, technical safeguard, physical safeguard that will clearly define policy and procedure to provide safety of patient information. It covers issues like- there must be supported proceedings in case if someone disclose health information without consent of patient, there must be a written set of policy procedure and designate a officer responsible for implementing the procedure, Policy must clearly define class of employees that are allowed to access Electronic Patient Health Information, access of equipment that contains sensitive information must be properly monitored and controlled, protect your system from direct view of public, before transmitting any information must ensure the authenticity of the other party.

(g) e-Business

Indian economy majorly based on e-business outsourcing. We need a privacy framework purely focused on e-business and cover privacy issues and provide legal assistance in case of any fraud, crime .Issues that are need to cover under privacy framework like proper storage of sensitive credentials like credit card, safe credit of money during online transaction, Confidentiality, Integrity availability, authentication of party must be ensured before beginning of transaction, Encrypt the data before transmission of sensitive information, Restrict access based on need to know basis, assign unique identification to the parties that are involved in the business for authentication purpose. Also maintain the policy that addresses e-business privacy.

(h) Tourism

India is the vast combination of heritage and culture. Due to this reason it generates most of the revenue 6.23% to the national GDP and 8.78% of the total employment in India from the tourism industry. When tourist visits in India they perform several transaction, but there is no guarantee that this provided information is not further misused.

Each tourist must have right that their information is protected, corrected, erased as per their wish. Employing the most appropriate physical and technical measures, staff training and awareness, to ensure that unauthorized access to, alteration or destruction of personal data does not take place. Similarly for the Medical Tourism the personal information of the patient must be protected. After the completion of the transaction the credit card information must be destroyed.

If such issues are covered in the privacy framework of the tourism then it must add on in Indian revenue, tourist feel safe while visiting the country, it also reduce the crime rate.

(i)National Security Surveillance

The collection of personal information by means of a surveillance system is lawful and justifiable as a policy choice, and if so, it must be ensured how privacy protective measures can be built into the system.

"*Reasonable expectation of privacy" is one of the keys to surveillance being legal.*

Using surveillance systems to address concrete, confirmed problems and/or incidents is acceptable only if the practice meets all statutory requirements. The activities like Access, Use, Disclosure, Retention, Security and Disposal of Surveillance Records must be regulated

- Prior to adopting a proposed surveillance program/practice an assessment of the impact on privacy is necessary.
- Public bodies should consider public consultations prior to introducing surveillance and inform those impacted once adopted.
- The design and operation of surveillance program/practice should minimize privacy intrusion to what is absolutely necessary to achieve its goals like designing and

installing Surveillance Equipment System operators require privacy-sensitivity training.

- For National Security purpose this definition assumes to be optimism. It's a matter of preserving national security, heritage, culture and life of each citizen. When we talk about national security with privacy concern then it is more focused on the safeguard of country sensitive information, agreement and security policies. Privacy of national security can be breached when espionage like activity can be performed by an individual to harm the reputation of the country.

With respect to national security there is exemption of privacy from it. Must have separate framework with proper defined national security privacy guidelines. It must include that the government has authority to investigate about any citizen, can seize any personal information regarding an individual when it mounts to National Security, because it is primary and foremost concern. Authority can access information anytime whether it belongs to private and public interest if they found susceptible or threat to national security. It has overall authority as it is deal with the preservation of millions of life.

Conclusion

The proposed system covers all domains in three dimensions legal, technical and political .In proposed system it has been tried to cover various domains as per present scenario, keeping the fast advancement in technology and emerging domains in the mind. The proposed system has given scope of advancement so that without interfering in other domains new domains can be added. The proposed system has been kept flexible and scalable so that not only present need but future needs can also be accommodated. Well structured framework for Privacy is definitely important for an individual but also for society as well as economical growth of country.