Cyber Crime Vis-À-Vis Violation of Massive Human Rights and Legislative Efficacy in India

Dr. Pramod J. Herode[1]

Abstract

Cyber crime is the phenomenon in the age of Information and Technology; neither has it geographical boundaries nor typological limit. The enormous growth in I.T. has closely intersected social life of an individual to such an extent that India stands at second number in the array of high numbers of users of internet. Under the garb of paper less governance, it is adopted as e-governance by public and private sectors. It has now close concern with right to privacy a basic human right of individual. Considering the wider amplitude of cyber crime legislative mechanism has been provided by the government as I. T. Act specifically enacted and certain provisions of IPC and Personal Data Protection Bill, 2019 are for additional support. However, epistemological data of ever increasing cyber crime shows inefficiency of legal framework at two places one efficacy of law and implementation of law. investigating agencies are not equipped with update knowledge and infrastructure, consequently victim is deprived of justice in consequence alarming situation is inevitably warrant for prompt and efficient legal and implementing mechanism which is sine qua non for public security.

Key words:*Cyber crime, I.T., Internet, Legal framework, Justice, E-governance, Privacy right.*

I. Introduction

Present era is known as an age of Information and Technology, as it has closely intersected all sphere of human life. Epistemological data authenticate that, information and technology is being used by members of present society as usual as it has become an essential commodity of their survival. However, their level of awareness of misuse or a crime pertaining thereto is lower. Undoubtedly, considering the magnitude of cyber crime and its impact on society, laws providing penal liabilities are enacted by the government. But in India the laws are seemed to be a matter of compliance of international obligation as cyber laws are ineffective in two ways namely, to combat the cyber crime on the one hand and to do justice to the victim on the other hand.

[1] Associate Professor, Dr. Ambedkar College of Law, Nagasenvana, Aurangabad. (M.S.)

Qualitative data proves that the graph of cyber crime is ever increasing and thereby life of individual as well as public is under imminent threat. This paper deals with a two aspects one is regarding legal framework and implementing mechanism available to deal with cyber crime and level of acquaintance of the law among the public is other. Magnitude of cyber is extremely wide, ranging from personal information of user to the property of individual everything is under the domain of cyber; hence, perpetrators are now committing crime through cyber and left traditional typology. In the domain of good governance it is inevitably required such efficacious law and implementing machinery as they would combat cyber crime, of course law and implementing machinery in isolation cannot achieve the goal unless they are supported by individual or public awareness.

II. Intersection Between I.T. and Privacy of Individuals in India

Rationale behind use of computer is multifaceted. One it is helpful for speedy disposal of assigned responsibility in the prevalence of pragmatic concept of global village and another is paperless administration so as to protect environment. The global mandate of e-governance compelled to the Indian government for adopting e-governance which procured changing facets of governance that is from manual to e-governance. It has brought about dynamic changes in documentation as well as official functioning both, consequently encouraged public out of necessity to become techno friendly. In the regime of privatization, e-governance has been implemented voluntarily by the stake holder as it is useful alternate to human resource and cost cutting. Similar scenario is equally visible in the public sector as well, it encompasses banking sector to defense department every public undertaking is under the domain of e-governance. Reportedly 'India stands at second number in the world for using internet having 12% users of total world, and China at first having 21% and America 8%'[2].

So far as privacy of data is concerned, 'I. T. Act was not comprehensive enough in all privacy dimensions as we were progressing to a digital economy and increased government measures focusing on personal information of citizens for

[2]VIJAY DARDA, DAILY LOKMAT, Nov.4, 2019.

reportedly percolating benefits, furthering national security versus privacy concerns/risks'[3]

By virtue of enormous revolution in information and technology Android mobiles are made easily available in the hands of individuals, users have now become netizens. Huge amount of individuals from younger to older irrespective of literacy background are became fond of social media. In order to have an access to social media, it requires to have Apps down loaded on the screen of handset, uncompromisingly, process of down loading APPS compels to provide full particulars of users. Upon compliance of filling up of information further access is allowed. This is usually a mechanical process. Now here comes a question of cyber security of your personal data as user is absolutely unaware of the future use or misuse of his or her information up loaded while downloading the APPs by the receiver. Astonishingly there is no assurance given from receiver about use or purpose behind asking this information is informed to the individual.

III. Gravity of the Problem of Cyber Crime

Slowly and steadily computer became an integral part of administration of public and private offices, and mobile with internet connectivity as part of life of individual. Therefore, numbers of users of it became high. Ranging from literate to illiterate, the problem of cyber crime has become of wide amplitude as it pertains to the quite larger section of the Indian society. Epistemologically speaking, 'with the ease of internet access, the numbers of social media users in India stood at 326. 1 million in India'[4]. Media wise data is also considerable and requires serious concern from the legal point of view as cyber crime is possible to be committed with them at any point of time. 'Face book now has 241 million active users in India—a million more than it does in U. S'[5]. You Tube is also not lagging behind in term of users, 'You Tube now has 265 million users in India

[3]BHUMESH VERMA, SAYANTAN DEY, UJJWAL AGRAWAL, *PRACTICAL EVOLUTIONOF DATA PRIVACY*, Lawyer,77(Feb. 2020) .
[4]www.statista.com accessed on 23. 1.2019 at 2.08 p.m.
[5]www.investopedia.com accessed on 23.102019 at 2.10 p.m.

on April 10, 2019'[6] . Case of data leakage by face book is known to everyone. The British Airways was imposed with the penalty of 22.9 million dollar.

So far as internet connectivity is concerned quite large size of population does use of it either private as well as public life, figures speaks, '34.4% of the population is internet users in India 2017. In 2018 India had 483 million internet users'[7]. Pre requisite condition for using internet-based services is to share user's personal information to be filled in without authentication of any security. In addition to this other Medias like Instragram, Twitter, WhatsApp etc. are also on the pick point of popularity in the Indian young as well as middle age population. Social media has quite extensive network either in rural as well as urban society both. It is immaterial whether users are literate or illiterate; in all sections of society use of social media is found to be at high level. It may also be a possibility that due to non acquaintance with the English language user may become victim of cyber crime. 'In India two users out of five are victims of cyber crime of any kind, when they came to know it at this point of time they are very late.'[8] Reportedly it is complained that, the mobile of Priyanka Gandhi was taped with the help of Israel software, Prafulla Patel was also victim of the same.

Considering this extensive network of use of cyber based Medias, perpetrators are attracted towards it and chosen means of commission of crime. Commission of cyber crime is easier than traditional crimes for multiple reasons. However, few of them are reproduced here, it requires no physical presence at the spot where it is committed, from any place it is possible, it requires very little physical labor and gain is comparatively high. As per governmental record the figures of cyber crimes are as under,

[6] www.hindustantimes.com accessed on 23.10.2019 at 2.18 p.m.
[7] www.statista.com accessed on 23.10,2019 at 2.13 p.m.
[8] VIJAY DARDA, DAILY LOKMAT, Nov. 4, 2019 .

Cyber crime registered under I. T. Act in the year 2016[9]

Publication /transmission of obscene/ sexually explicit act, etc in electronic form	u/s 67A	U/s 67B	u/s 67C	U/s 72&72A	Other cyber crimes under IT Act	Total cyber crimes under IT Act
957	930	17	10	35	713	8613

Cyber crime registered as per IPC (involving computer as a medium) 2016[10]

Theft Of data	Criminal breach of trust/fraud u/s 406,408,409	Debit card /credit card	Others	Cheating	Forgery	Counterfeiting	False Evidence/ Destruction Of electronic record for evidence u/s 193,204	Other IPC Cases	Total cyber crime
86	56	26	30	2329	79	10	06	950	3518

IV. Need of Protective Legal Mechanism

In India, to enact Information and Technology Act, 2000 is one sort of compliance done of the international obligation. UNO being apex international body has played active role by taking initiative to frame UNICITRAL model law to assure safety by legislative mechanism to I. T. users. India being member state of UNO it was obligatory on its part to have such law in prevalence which would deal aptly with cyber crime or crime relating to information and technology, therefore based on the UNICITRAL model law on International Commercial Arbitration recommended by the General Assembly of UNO by its resolution on dated 30th January 1997 the Information and Technology Act, 2000 has been enacted. After coming across with shortcomings necessary consequential amendments have also been carried out in Indian

[9] National Crime Research Bureau Report 2016.

[10] Ibid.

Evidence Act so as to maintain its efficacy in present substantive and procedural types of law.

V. Cyber Laws vis-à-vis Information and Technology Act, 2000

Considering the gravity of cyber crimes a special Act that is Information and Technology Act, 2000 has been enacted by the government by having hand in glow with international instrument. It is pertinent to mention that, I. T. Act 2000 has two significant features; first, it has for the first instance recognized a fact that, in the digital world, modalities of commission of crime are different and that is cyber crime, and second it provides punishment for commission of such crime. Of course, cyber crime is such phenomenon which has far greater detrimental repercussions on larger public life than traditional crimes as it has covered larger area of life of individuals particularly privacy of individuals in India. Upon considering it seriously; this Act has laid down rigorous punishment for cyber crimes respectively defined in it. Accordingly there are different offences made punishable under I. T. Act 2000 and I. P. C. as well.

VI. Cursory Review of Penal Provisions Regarding Cyber crimes under I.T. Act 2000 and other Penal Laws

I. T. Act, 2000 being enacted to deal with cyber crime is earmarked specifically as cyber law because of its outstanding feature that it possesses identity of special piece legislation. Whole thrust of combating cyber crime is on this Act. Let us recapitulate few among the others offences made punishable in I. T. Act, 2000 are reproduced here namely, tampering with computer source documents under section 65, however, in order to understand the ambit of this section the court incase of Syed Asifuddin's[11]court laid down that Tampering with source code attracts section 65 of I. T. Act 2000.The facts of this case are the accused were employees of the Tata Indicom co. charged for manipulation of the electronic 32-bit number (ESN) programmed into cell phones which were exclusively franchised to Reliance Infocom.

[11] 2005 Cr. L. J.4314, decided by A. P. High Court on 29th July 2005.

Hacking with computer systems, data alteration made punishable under section 66 the best example worth quoting is of the case of hacking official website of Maharashtra State Government, it was hacked by Hackers Cool-Al-Jazeera, accused were from Soudi Arabia. Geographically far away from India, but through I. T. modes offence could take place.

Publishing obscene information under section 67 the punishment for first time is imprisonment which may extend to five years and fine up to one lakh for subsequent time imprisonment which may extend up to ten years and fine up to rupees two lakhs. The leading case is 'The Sate of Tamil Nadu Vs SuhasKatti'[12], the accused was known family friend of the victim and interested to marry with her, but she got married with other and subsequently break down of marriage wedlock of her was also took place, accused being interested in marrying with her started contacting her but she was reluctant, hence he started harassing her through internet, accused was tried and punished u/s 469, 509 of IPC and 67 of IT Act. This case is considered as the first case wherein accused was convicted under Sec 67 of I. T. Act 2000 in India.

Unauthorized access to protected system under section 70 pertaining to this section, in case of Frios VS State of Kerala[13], the facts of this case that, it was declared the FRIENDS application software as protected system. The author of the application challenged the notification and the constitutional validity of software under section 70, the court upheld the validity of both, and laid down that, Tampering with source and destroying the source code are punishable with three years jail and two lakhs rupees fine for altering, concealing and destroying the source code, causing breach of confidentiality and privacy under section 72 in this context stern step has been taken by the Government of India by preparing the Personal Data Protection Bill, 2019 it was placed of the floor of Lok Sabha on 11.12.2019. Clause 3 of this Bill defines the word "anonymisation". It brings public and private sectors under the tenet of data security. Publishing false digital signature certificates under section 73 Bennett Coleman & Co. VS Union of India[14], in this case publication has been explained as the 'publication means dissemination and circulation' in the digital era, the term publication includes transmission or data in electronic form.

[12] Decided by the chief Metropolitian Magistrate, Egmore, on 5th Nov. 2004.
[13] A.I.R. 2006 Kerala 279 (India).
[14] 1972 (2) S.C.C. 788 (India).

In addition to these sections, certain sections of IPC are also aptly dealt with cyber crimes, these are as under;

Sending intimidating massages through e-mail under section 503, sending defamatory messages by e-mail under section 499, forgery of electronic records under section 463 and creating bogus websites and committing cyber frauds under section 420, committing e-mail spoofing under section 463, committing web-jacking under section 383, causing e-mail abuse under section 500. In addition to this certain provisions of Narcotic Drugs and Psychotropic Substances Act 1985 and online sale of arms is punishable under Arms Act 1959. This is legal mechanism made available in India to deal with cyber crime. The legal provisions give definitions of offence and punishment for commission of these offences, despite of it; these laws have not created remarkable impression in combating the cyber crime in India.

VII. Personal Data vis-à-vis Protection of Human Rights

Close intersection between human life and use of information technology has generated new discourse regarding violation of human right. As discussed above, receiving personal data for using certain apps or I. T. Services is pre requisite condition. The reported cases regarding misuse of personal data have necessitated thinking on it from the human rights perspective.

i. Universal Declaration of Human Rights, 1948

The Universal Declaration of Human Rights 1948 was resolved by the General Assembly of United Nations Organisation on 10th December 1948. Article 12 provides that, 'no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference of attacks'[15]. The corresponding provision is found under Article 21 of the Constitution of India. it is a contribution of the Indian judiciary to widen the ambit of this article and bring right to privacy in the ambit of fundamental right.

[15] DR. A. N.SEN, *HUMAN RIGHTS*,554, SRI SAI LAW PUBLICATIONS, Faridabad. (2012).

In the background of emerging globalization during 1980s the possibility of data traversing had created necessity to have regulation, 'this resulted in the OECD (Organisation for Economic Cooperation and Development) to formulate the 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data'[16].

ii. Personal Data Protection Bill, 2019

Considering the gravity of data protection the in '*K. S. Puttaswamy vs. Union of India*'[17] Supreme Court of India recommended as a need of time to have special legislation for protection of the data or right to privacy, having regard to this, a committee under the Chairmanship of Justice B. N. Srikrishna was set up, it recommended positively. Hence, as result, The Personal Data Protection Bill 2019 came into existence, which was introduced in the Loksabha on 11.12.2019. It has pioneer feature that it has tune with European Union's General Data Protection Regulation (GDPR). The main object of this Bill is to regulate the data of Indian Citizens. Having synergy with digital economy where personal data of individual is used as commodity has created to have special legal framework. It is a sincere endeavor of the legislature to provide rights and remedies to Indian citizens for protection of its rights.

However, it appears to have covered vague provisions, "most of the provisions lack clarity and proper enforcement mechanism, which if passed as an Act, would end up increasing volumes of petitions and most certainly be raising questions regarding the security of an individual's personal data"[18]. The rays of hope of strong protection of data of an individual again set down.

iii. I.T. Act 2000 and Posthumous Scenario of Cyber Crime in India

Present era is known as era of rule of law, in this background it is reasonably expected that, I. T. Act, 2000 must be an effective instrument in extending protection from potential threat of cyber crime and bringing perpetrators to the door of guilt. However, it is a legitimate expectation that when special law is meant for combating cyber crime, it should restrict rather reduce rate of

[16]BHUMESH VERMA, SAYANTAN DEY, UJJWAL AGRAWAL, *PRACTICAL EVOLUTIONOF DATA PRIVACY*, Lawyer,75(Feb. 2020) .
[17] (2017) 10 S.C.C. 1(India) .
[18]SHUBHODIP CHAKRABORTY, *PERSONAL DATA PROTECTION BILL, 2019-A CRITICAL ANALYSIS:OLD WINE IN NEW BOTTLE* 241 Practical Lawyer 69(Feb. 2020).

commission of crime. But in case of cyber crime total paradoxical reality is visible, as the graph of cyber crime is ever increasing. The data published by government agencies exposes factual realities of offences occurred and accused arrested. Statistical data indicates that, cyber crime cases in India registered under the IT Act, 2000 have increased at the rate of 300% from 2011 and 2014[19]. In 2015 there were 11,592 cases of cyber crime registered in India[20]. These figures are of reported cases, but due to lack of awareness regarding legal mechanism available for combating cyber crimes to the victims most of the cases are remained unreported to the appropriate authority hence they are not included in this figure. It means actual numbers of cases are higher than the shown numbers. In addition "in the report of the Norton Cyber Security Insight it is revealed that, in 2017, Rs. 18.5 Dollar have lost by victims of cyber crime in India"[21]. The worth quoting unique feature of perpetrator in cyber crime is, it is accomplished by either individual alone or by group. The high quantity of gain has attracted to get indulged into cyber crime to certain corporations i. e. artificial persons. Modality of commission crime by corporation has posed challenges in front of available traditional legal as well as investigating mechanism as the criminal liability is individual centric in our prevailing laws including I. T. Act. This scenario confirms *ipso facto* the alarming situation in India which solicits such legal framework containing stringent provisions of punishment. Undoubtedly, it is legal mechanism with efficient implementing agencies can reduce rate of cyber crime and give appropriate relief to the victims.

VIII. Cyber Crime and Efficacy of Investigating Agencies in India

Certainly on papers government has established cyber cells as separate investigating agencies to probe into cyber crime, but, in terms of efficiency they are not performing up to minimum level of reasonable expectation. man may lie but fact does not, during the course of personal interview of Adv. S. S. Quasi[22], that, he used his ATM card for making payment of lunch on the hotel counter,

[19] ECONOMIC TIMES, Bennett, Coloman&Co. Ltd, May 8, 2017.
[20] NATIONALCRIMERESEARCHBUREAU, LineMint. H.T. Media Ltd., May 8, 2017.
[21] VIJAY DARDA, DAILY LOKMAT, Nov. 4, 2019.
[22] Practicing lawyer at High Court of Judicature Bombay, Bench at Aurangabad (M.S.).

immediately after half hour Rs. 70,000/- were reported to be withdrawn from his account, he immediately reported the matter to the police, initially place of withdrawal was traced, but tracing accused and recovery of money is yet to be done when one month period of time is over. He approached to the police but, typical reply was given by the police as 'investigation is in progresses'. This case is quoted as representative example, there are myriad of cases wherein no investigation is culminated with fruitful results. This empirical case is worth generalizing to draw an inference of inefficiency of investigating agencies in cases like cyber crimes vis-à-vis violation of human rights. On the contrary 'Vijay Darda has shared information that, his son was serving in America, cyber criminals stolen away all amount from his bank account, he reported the incident to the bank, a speedy investigation was culminated into return his amount within eight days'[23]. The narration of both cases necessitated comparison to draw inference as to how legal and investigating mechanism is efficient in India in dealing with cyber crime.

Supporter may say that investigating agencies are well equipped with investigating tools in cyber crime but, reality is extremely harsh. Ordinary police personals are ineligible to investigate into cyber crime as it unavoidably requires cyber expertise. The factual data reveals the background of investigation officer in cyber crime. Majority of the cases are investigated by such police officers those who lack expertise in the field of cyber technology prevailing in up dated version at present.

IX. Conclusion

Cyber crime is a phenomenon which has now become great threat to security of public life either common or individual at large which otherwise amount to violation mass human rights in the realm of globalization. Comparatively level of awareness regarding cyber crime is in the public irrespective of socio-educational background is extremely lower as it is totally a technical functioning which requires expertise in it. On the contrary perpetrators are comparatively highly experts in technological dealings of cyber related issues. The way cyber crime is committed is beyond reach of understanding of man of ordinary

[23]VIJAY DARDA, DAILY LOKMAT, Nov. 4, 2019.

prudence or man who is illiterate in cyber related technologies. The ambit of adverse consequences on public are comparatively higher than traditional crime as it ranges from property to personal details everything is subject matter of cyber crime. So far as legal framework is concerned it lacks efficacy in combating or controlling cyber crimes, particularly, data protection is concerned law is ineffective as compare to western legal framework. Therefore, it requires serious attention either of the legislature as well stake holders. Undoubtedly it has become issue of international concern but India as such it has created alarmingly dangerous situation, it has posed threats to every sections of public as well as individual life. Hence it calls for certain more drastic steps either in legal framework which provide stringent punishment or in implementing mechanism equipped well with highly qualified resource persons and infrastructure. In addition to this, public program aiming at generating public awareness regarding cyber crime need to be conducted which would help in up grading the level of acquaintance with cyber crime. Such programs may act as; 'prevention is better than cure' and would help to restrict a public to become a victim of cyber crime. data protection must be treated as human rights protection of Indian citizen, such inculcation ought to be done by public programs in India.