RIGHT TO PRIVACY IN CYBERSPACE: A COMPARATIVE ANALOGY BETWEEN INDIA AND USA

Sudeshna Halder, Amity University, Kolkata

ABSTRACT

The arena of the fundamental rights has been enlarging since its incorporation in the Constitution of India are made for the protection of the citizens' rights. When compared to the protection of the citizens' rights in cyber space there is much lacuna for effective laws relating to the right of privacy in cyberspace. This article envisions the importance of privacy rights of internet users in cyber space.

Just as Article 21 of the Indian Constitution depicts right to privacy of any citizen of India, therefore the Information Technology Act, talks about right to privacy in cyber space and combat other crimes too like hacking, Cyber Stalking, Cyber Pornography, etc. In this article, importance of Cyber laws is described as to why the laws of the Information technology has to very efficient to combat all new emerging crimes in cyberspace.

USA being the cradle of technology, so laws pertaining to combat cybercrimes are very efficient in the nation includes various Acts like Cybersecurity Information Sharing Act, National Cybersecurity Protection Advancement Act of 2015, etc.

Nations are constantly trying to combat the new age cybercrimes by amending the existing laws. Internet usage is so intertwined with every aspect of human life that it has become inseparable. Therefore, cyber laws have to be potent to protect individuals from any cybercrimes.

Keywords: Cyber space, cybercrimes, Information technology, Internet, Privacy.

Introduction

The very fundamental rights enshrined in our Indian Constitution depicts various rights viz. right to equality, protection of life and personal liberty, right to freedom of which the right to privacy has in this era of advancement of technology. The Constitution has not guaranteed the 'right to privacy' as a fundamental right to the citizens of India but the Supreme Court of India has construed the 'right to privacy' as a part of the Article 21[1] i.e., right to 'protection of life and personal liberty'.

Privacy is an important aspect which indicates the state of being free from public attention. The term 'right to privacy' as confirmed by the Supreme Court that it is a fundamental right which can be derived from Articles 19[2] and 21 of the Constitution of India and need not required to be enumerated separately. Right to privacy being a natural right exists as an essential part to the right to life and liberty. The right to privacy being the fundamental and inalienable right to every individual embraces all data and information.

Article 19 of the Constitution embraces the judgment of the Supreme Court of India recognizing the right to privacy under Indian Constitution.

Cybercrimes are increasing at such an alarming rate that the protection of data and information of every single person using the internet have to be protected from being infringed.

It protects an individual from the scrutiny of the State in their home, of their movements and over their reproductive choices, choice of partners, food habits, etc. Therefore, any action by the State that results in an infringement of the right to privacy is subject to judicial review. The 20th century world has developed not only in economies, legal field, standard of living, technology, culture, education but also in the field of internet and information technologies. With the advancement of time, the internet users are highly exposed to the risk of privacy of person is somewhat compromised risk of privacy in cyberspace.

[1] Indian Constitution, Article 21
[2] Indian Constitution, Article 19

Cyberspace and Privacy

In the era of technology advancement, the present-day world has almost all the people are internet users. Cyberspace is the ever growing exponential and dynamic space expression for web of computers, communication networks, and electronics. Cyberspace refers to that medium of computer networks or an electronic system that allows computer users around the globe to communicate with each other or to access information for any purpose.[3] It denotes to the virtual world where an electronic medium is used to facilitate online communication and networking among individuals around the globe. Google, Facebook, Yahoo are the examples of the cyberspace. In this cyberspace, there exists personal data and information of every internet user and which are likely to be exposed by other people involved in illegal activities. There are cyber laws which are formulated for to ensure the protection from any kind of infringement risking the exposure of the privacy of personal information of the individuals present in cyberspace. Thus, the protection of the privacy of people in cyberspace is ensured by the cyber security laws. The individuals who are using the social networking sites which are used extensively social interactions for uploading their personal content, has further aggravated the issue of internet privacy. On one hand, privacy is an incident of fundamental freedom or liberty whereas the right to privacy is one of the basic Human rights provided to an individual.

INTERNATIONAL ASPECT:

More technical expertise is required in cybercrime investigations than conventional crime as well as it should be ensured that conventions are enacted for protection of fundamental privacy principles both in the national and international law. There are international declarations that are widely recognized as the basis for the protection of privacy and personal life. **United Nations Human Rights Council, 2006** has stated that the freedom of expression and information under Article 19 of the of the **International Covenant on Civil and Political Rights (ICCPR),** 1976 that 'Everyone has the right to freedom of opinion and expression; this right includes freedom to

[3] https://dictionary.cambridge.org/dictionary/english/cyberspace, (last visited Dec 22, 2023, 03:53 P.M.)

hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers[4]'

CYBER-CRIMES:

- ***Hacking*** – When any unauthorized user attempts to or gains access to an information system is known as a hacker followed by demand of ransom as found in banks, hospitals, or personal devices. Therefore, hacking is a cybercrime even if there is no visible damage to the system though it is an invasion in to the privacy of data.

- ***Cyber Stalking*** – Cyber stalking involves use of internet to harass someone. The behavior includes false accusations, threats etc. Normally, majority of cyber stalkers are men and most victims are women.

- ***Identity theft***: It is the piracy or infringement of identity in cyberspace when one uses other's personal identifying information viz. name, personal pictures, debit or credit card number. etc., without their permission for fraudulent or malicious practices.

- ***Cyber Pornography*** – With the increasing approach of internet to the people, there is also an increase in the victimization of Women and children for sexual exploitation through internet. Pedophiles (a person 16 years of age or older who is primarily or exclusively sexually attracted to children who have not begun puberty) use the internet to send photos of illegal child pornography to targeted children to attract them to such fun and later they are sexually exploited for gains.

- ***Phishing*** – when cybercriminals send fraudulent emails pretending it to be from authenticate purposes and thereby collect important personal information.

- ***Software Piracy*** – It is an illegal reproduction and distribution of software for business or personal use. This is a type of infringement of copy right and a violation of a license

[4] Universal Declaration of Human Rights - the United Nations. https://www.un.org (last visited Dec 22, 2023, 03:53 P.M.)

agreement. Since the unauthorized user is not a party to the license agreement it is difficult to find out remedies. There are numerous cases of software piracy.

- ***Patent infringement, Social-media fraud, cyber spying, banking fraud, etc., are prevalent types of cyber-crimes.***

In **U.S. vs. Joseph C. Bledsoe**[5] the defendant was convicted for knowingly publishing a notice over the Internet offering to exchange child pornography in violation of 18 U.S.C. S. 2251(d) the U.S. Court of Appeals for the Fourth Circuit affirmed the conviction and sentence.

The Right to Privacy is one of the most esteemed rights for human being while valuing the importance of this right. The human beings by their very nature require a space exclusive from interference of any kind. This is necessary for the development of their individual personality. This right has acknowledged recognition and protection in societies of all times. In modern times, the human right movements have considerably affected the concept and jurisprudence of legal rights. The right to privacy has found unequivocal mention in all international instruments concerning human rights[6]. In India, the right to privacy has received immense protection as fundamental right under the Constitution of India.

Alan Westin (1967) in 'Privacy and Freedom' defined privacy as the "desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and their behavior to others."[7]

Data and personal information shared in internet is very significant aspect in today's world and threat to privacy over internet is something which is unavoidable threat. There are strong and effective security measures adopted by the developed countries when information technology is firmly rooted amongst the masses of the citizens of that nation. As a result of this any issues or disputes can be redressed effectively to a much considerable extent. Cybercrimes are now-a-days

[5] U.S. vs. Joseph C. Bledsoe 04-4276, 177 Fed Appx. 311(last visited Dec 22, 2023, 03:53 P.M.)
[6] International Covenant on Civil and Political Rights, Article 17
[7] Alan F. Westin, Privacy And Freedom, 25 Wash. & Lee L. Rev. 166 (1968)
http://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20 (last visited Dec 22, 2021, 04:06 P.M.)

increasing at an alarming rate that cybercrime investigations need to handle the account privacy concerns while implementing the procedural provisions of the convention on cybercrime.

Cyber laws and its comparative study between India and USA

Invading the privacy of any person in daily course or in digital space is not at all encouraged and is strictly a punishable offence any country of the world whether it is India, USA, European countries, etc.

In INDIA:

Emergence of right to privacy as fundamental right of the Indian Constitution:

- In **MP Sharma & Ors. vs Satish Chandra**, the 8-judge bench of the Supreme Court held that the drafters of the Constitution did not intend to subject the power of search and seizure to a fundamental right of privacy. They opined that the Constitution does not include language like the Fourth Amendment of the US Constitution, and found no justification to import the concept of a fundamental right to privacy in search-and-seizures, through what they called a 'strained construction[8]'.

- In **Kharak Singh v State of Uttar Pradesh 1962**, the right to privacy was applied here to challenge the surveillance of an accused person by the police. Kharak Singh then challenged the constitutional validity of Chapter XX of Constitution and the powers conferred by it on police officials, since it violated his fundamental rights under Article 19(1)(d) i.e., right to freedom of movement and Article 21 i.e., protection of life and personal liberty. The 6-judge bench held that domiciliary visits at night was unconstitutional, but upheld the rest of the Regulations. More importantly, the bench held that the right of privacy is not a guaranteed right under the Constitution.

[8] Supreme Court Observer, https://www.scobserver.in/journal/right-to-privacy-court-in-review/#:~:text=MP%20Sharma%20v%20Satish%20Chandra&text=In%20M.%20P.,a%20fundamental%20right%20of%20privacy. (last visited Dec 22, 2021, 04:06 P.M.)

- In **R. Rajagopal vs. State of Tamil Nadu**[9] which is otherwise known as the 'Auto Shanker Case,' the Supreme Court of India has held that the right to privacy or the right to be let alone is guaranteed by Article 21 of the Constitution of India. The Supreme Court of India ruled that a magazine had a right to publish an autobiography written by a prisoner, even without his consent or authorization and the Apex court explained that it was important to strike a balance between the freedom of the press and the right to privacy, and found that the state and its officials do not have the right to impose prior restraints on the publication of materials that may be defame the State.[10]

A citizen has a right to safeguard to privacy of his own, his family, marriage, and education among other matters. No one can publish anything without the consent of the any individual whether truthful or otherwise and whether laudatory or critical. If any individual does so, he would be violating the right of the person concerned and would be liable in action for damages. However, the position would be differed if he voluntarily puts into controversy or voluntarily invite or raises a controversy.

Cyber laws in India is an amalgamation of Contract, Intellectual property, Data protection, and privacy laws. With the Computer and internet taking over every aspect of our life, there was a need for strong cyber law. Cyber laws supervise the digital circulation of information, software, information security, e-commerce, and monetary transactions.

It is the courts in India that have admitted the right of privacy in cyberspace as a status of fundamental right in Article 21, though it is not directly provided in the Constitution of India.

The Information Technology Act, 2000 enshrines the cyber laws and is capable of the gamut of cybercrimes. Computer technology, mobile devices, software, and the internet are both medium and target of such crimes. All Traditional criminal activities are such as theft, fraud, forgery,

[9] R. Rajagopal vs. State of Tamil Nadu (1994) 6 SCC 632
[10] Global Freedom of Expression, https://globalfreedomofexpression.columbia.edu/cases/r-rajagopal-v-state-of-t-n/#:~:text=The%20Supreme%20Court%20of%20India,auto%2Dbiography%20was%20not%20published. (last visited Dec 23, 2021, 04:06 P.M.)

defamation, and mischief are part of cyberspace. These were addressed in the Indian Penal Code already.

The laws Information Technology Act, 2000 elucidates legal recognition to any operation completed by electronic exchange of data and other electronic means of communication or electronic commerce transactions. After the enactment of the above Act there was further amendment in Indian Penal Code, 1860, the Evidence Act 1872, the Bankers' Books Evidence Act 1891, and the Reserve Bank of India Act 1934. The aims of the Act are as follows:

- To grant legal recognition to all transactions completed via electronic exchange of data or other electronic means of communication or e-commerce, in place of the earlier paper-based method of communication,
- To give legal recognition to digital signatures for the authentication of any information or matters requiring legal authentication,
- To aid the electronic filing of documents with Government agencies and also departments
- To give legal sanction and facilitate the electronic transfer of funds between banks and financial institutions,
- To grant legal recognition to bankers under the Evidence Act, 1891 and the Reserve Bank of India Act, 1934, for keeping the books of accounts in electronic form.

Aadhaar Data Breach Case– The Supreme Court in Justice K.S. Puttaswamy vs. Union of India[11] 2017, unanimously affirmed that the right to privacy is a fundamental right under the Indian Constitution. The Indian Government was collecting and compiling both the demographic and biometric data of the residents of the country to be used for various purposes in the Aadhaar Card Scheme of the Government of India. This data of residents of India that was collected various times where there was violation of right to privacy. The legal position regarding privacy was very doubtful. The impermissible and divergence of opinion commenced with the judgment of Supreme

[11] Justice K.S. Puttaswamy vs. Union of India Writ Petition (CIVIL) NO 494 OF 2012

Court decided by the smaller benches of two or three judges in Gobind v. State of MP[12], R. Rajagopal v. State of Tamil Nadu[13] and Peoples Union for Civil Liberties v. Union of India.[14] Such divergence of opinion was also submitted by the counsel of one of the respondents.

The Court by an interim directed the Union of India to give wide publicity in the electronic and print media including radio and television networks that it was not mandatory for a citizen to obtain an Aadhaar Card not to be a condition for obtaining any benefit otherwise due to a citizen. The Aadhaar number which is also known Unique Identification Number would not be used by the respondents for any purpose other than PDS Scheme and in particular for the purpose of distribution of food grains, etc. and cooking fuel, such as kerosene and LPG distribution Scheme.[15] The biometric data, unlike the UIDAI's statement, is not the only privacy concern with this breach but as well as the disclosure of demographic data, such as an individual's name, date of birth, address, PIN, photo, phone number, e-mail, etc. is not any less of a privacy concern. This data forms the basis of many cybercrimes, be it identity theft, etc. When obtaining biometric data is getting simpler, such as the extraction of fingerprints from photographs or the spoofing of iris scans then, it is becoming a huge target for cybercriminals as obtaining biometric data will be available from any Aadhaar card number once they get all the credentials pertaining to that, and because of the potential of combining it with the troves of other information already illegally available. Therefore, it is extremely dangerous to underrate the value of the data disclosed in this breach, simply because it did not include biometric data.

A data 'breach' is not defined under the Indian Information Technology Act, 2000 or the Aadhaar Act, 2016. However, a data 'breach' is not limited to a technical breach like hacking the security systems of the Central Identities Data Repository (CIDR), as is commonly understood. When gaining unauthorized access to a database in this case, possibly the CIDR it is very much a data breach and a violation of privacy. It is the seriousness of this act of gaining unauthorized access to

[12] Gobind v. State of MP AIR 1975 SC 1378
[13] R. Rajagopal v. State of Tamil Nadu (1994) 6 SCC 632
[14] Peoples Union for Civil Liberties v. Union of India AIR 1997 SC 568
[15] Per J. Chelameshwar, S.A. Bobde and C. Nagappan

the Aadhaar database, which makes it punishable not only under Section 43[16] of the IT Act but also under Section 38 of the Aadhaar Act itself.

American whistleblower Edward Snowden delivered a firm reproof to the Indian government for "destroying the privacy" of its citizens and spoke out in support of the reporter who broke the Aadhaar data breach.

So important provisions of Information Technology Act, 2000 are as follows:

- Trying to tamper with computer resources[17]- Section 65
- Trying to hack into the data stored in the computer[18] – Section 66
- Provision of penalties for misappropriation of information stolen from computer or any other electronic gadget[19] – Section 66B
- Provision of penalties for stealing someone's identity[20]-Section 66C
- Provision of penalties for access to personal data of someone with the help of computer by concealing their identity[21]- Section 66D
- Provision of penalties for breach of privacy[22]- Section 66E
- Provision of penalties for cyber terrorism[23]- Section 66F
- Provisions related to the publication of offensive information[24]-Section 67

[16] The Information Technology Act, 2000, Section 43 (09 of 2000) Acts of Parliament, 2000 (India)
[17] The Information Technology Act, 2000, section 65, (09 of 2000) Acts of Parliament, 2000 (India)
[18] The Information Technology Act, 2000, section 66, (09 of 2000) Acts of Parliament, 2000 (India)
[19] The Information Technology Act, 2000, section 66B, (09 of 2000) Acts of Parliament, 2000 (India)
[20] The Information Technology Act, 2000, section 66C, (09 of 2000) Acts of Parliament, 2000 (India)
[21] The Information Technology Act, 2000, section 66D, (09 of 2000) Acts of Parliament, 2000 (India)
[22] The Information Technology Act, 2000, section 66E, (09 of 2000) Acts of Parliament, 2000 (India)
[23] The Information Technology Act, 2000, section 66F, (09 of 2000) Acts of Parliament, 2000 (India)
[24] The Information Technology Act, 2000, section 67, (09 of 2000) Acts of Parliament, 2000 (India)

- Provision of penalties for publishing or circulating sex or pornographic information through electronic means[25]- Section 67A

- Publication or broadcast of such objectionable material from electronic means, in which children are shown in obscene mode[26] – Section 67B

- In **Tanaya Mukherjee v. Amit Kumar Sen**,[27] Adjudicating Officer of West Bengal held the respondent liable for accessing and extracting the complaint's mobile phone and its content without her knowledge and consent and awarded compensation of Rs. 50,000/- to the complainant.

- In **JCB India Ltd. v. Abhinav Gupta**,[28] the petitioner had accused the respondent o data theft and copyright violations and was held guilty by the court.

The laws envisaged in Indian Penal Code, 1860 and Evidence Act, 1872 are therefore the punishments for the crimes which are elucidated in Information Technology Act, 2000. Now, Information Technology (Amendment) Bill 2006 was amended by Information Technology Act Amendment Bill 2008 This new amended act came up with a much broader and precise law on different computer-related crimes and cyber offenses committed in cyber space.

The Indian Central Government passed the Digital Personal Data Protection Act (DPDP) in 11th August 2023 which aims to protect data principles and limit the activities of data fiduciaries. This Act aims to include:

- new broad definitions of data principles, data processor, consent manager, significant data fiduciary, etc.

- Consent management, cross-border data transfers, data protection impact assessments, data protection officer appointment.

[25] The Information Technology Act, 2000, section 67A, (09 of 2000) Acts of Parliament, 2000 (India)
[26] The Information Technology Act, 2000, section 67B, (09 of 2000) Acts of Parliament, 2000 (India)
[27] Tanaya Mukherjee v. Amit Kumar Sen Complaint No. 1 of 2014
[28] JCB India Ltd. v. Abhinav Gupta October 15, 2010

Thus, the DPDP Act 2023 in conformity with General Data Protection Regulation of European Union and California Consumer Privacy Act of 2018 is to ensure concerns about data breaches in Indian territory.

In USA

The USA opines that cyberspace as an integral component of all facets of American life, including their economy and defense[29]. This nation being the cradle of the Internet and a superpower in the cyber realm, USA was also among the first to discover the lethal threats that lay intertwined in World Wide Web.

In **U.S. vs. Aaron Reed Hinton**,[30] the accused were charged for the receipt of child pornography through the mails in violation of 18 U.S.C. S. 2252(a)(2).

There has been constant effort to strengthen its cyber security laws, the federal government is introducing several new cyber security laws as well as amending the older ones for a better security ecosystem. Below are a few of them:

- **Cybersecurity Information Sharing Act (CISA)**[31]: the aim of is to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes. The law allows the sharing of Internet traffic information between the U.S. government and technology and manufacturing companies. The bill was introduced in the U.S. Senate on July 10, 2014, and passed in the Senate October 27, 2015.

- **Cybersecurity Enhancement Act of 2014**[32]: It was signed into law December 18, 2014. It provides an ongoing, voluntary public-private partnership to improve cybersecurity and

[29] The White House, 2018, National Cyber Strategy for USA. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf, (last visited Dec 23, 2021, 04:50 P.M.)
[30] 06-4017, 236 Fed. Appx. 237
[31] A Glance At The United States Cyber Security Laws – Appknox, https://www.appknox.com/blog/united-states-cyber-security-laws, (last visited Dec 23, 2021, 04:50 P.M.)
[32] A Glance At The United States Cyber Security Laws – Appknox, https://www.appknox.com/blog/united-states-cyber-security-laws, (last visited Dec 23, 2021, 04:50 P.M.

strengthen cybersecurity research and development, workforce development and education and public awareness and preparedness.

- **Federal Exchange Data Breach Notification Act of 2015**[33]: This bill requires a health insurance exchange to notify each individual whose personal information is known to have been acquired or accessed as a result of a breach of security of any system maintained by the exchange as soon as possible but not later than 60 days after discovery of the breach.

- **National Cybersecurity Protection Advancement Act of 2015**[34]: This law amends the Homeland Security Act of 2002 to allow the Department of Homeland Security's (DHS's) national cyber security and communications integration center (NCCIC) to include tribal governments, information sharing, and analysis centers, and private entities among its non-federal representatives.

- **The Data Protection Act of 2021**[35], which would create a new federal agency to protect Americans' data. The USA territory takes proper initiative that concerns data privacy, net neutrality, cyber-security, and fairness in data usage as mentioned in Cybersecurity Legislation 2021[36].

USA President Joe Biden and VC K. Harris announced the National Cybersecurity Strategy in USA with the objective to enhance:

- Defend Critical Infrastructure
- Disrupt and Dismantle Threat Actors
- Shape Market Forces to Drive Security and Resilience

[33] Ibid 32.
[34] A Glance At The United States Cyber Security Laws – Appknox, https://www.appknox.com/blog/united-states-cyber-security-laws, (last visited Dec 24, 2021, 12:50 P.M.)
[35] Ibid 34.
[36] Cybersecurity Legislation 2021 - National Conference of State, https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2021.aspx, (last visited Dec 24, 2021, 12:55 P.M.)

- Invest in a Resilient Future
- Forge International Partnerships to Pursue Shared Goals[37]

The State and Local Government Cybersecurity Act of 2021 is designed to improve coordination between the Cybersecurity and Infrastructure Security Agency (CISA) and state, local, tribal, and territorial governments. the Federal Rotational Cyber Workforce Program Act of 2021, U.S. government employees in IT, cybersecurity, and related fields will be able to rotate through roles across agencies, enabling them to gain new skills and experience in a variety of job functions.[38]

Importance of Cyber laws

Due to the vast enhancement of digitalization along with globalization internet usage has become intertwined with everything in every aspect. People spend more time in cyberspace in relation to trade, business, gaming, promotion purposes, etc. and it inevitable that cybercrimes will be present and to combat that Cyber laws in every nation should be present. Cyber law in India is important because of the prime reason that cybercrime act in India encompasses and covers all the aspects which occur on or with the internet - transactions, and activities which concern the internet and cyberspace. For instance, Tapping is a serious invasion of an individual's privacy as held in "People's Union of Civil Liberties v. Union of India and Anr,[39] which could only be prevented with these cyber laws. "The Cyber Laws in India has paved the way for electronic commerce and electronic governance in the country by ensuring maximum connectivity and minimum cyber security risks. Also, enhancing the scope and expanding the use of digital mediums," says Advocate Krishnamohan K. Menon. It was quite a long time that India has no law governing cyber laws involving privacy issues, jurisdiction issues, intellectual property rights and a number of other legal issues. To augment benefits of ICTs and secure confidence of user's information society should be safe and secured not only through cyber laws per se but also appropriate enforcement

[37] Biden-Harris Administration, The White House (.gov), https://www.whitehouse.gov (last visited Dec 24, 2021, 12:55 P.M.)
[38] EC-Council_Cybersecurity-Exchange-tab, https://www.eccouncil.org/cybersecurity-exchange/executive-management/federal-cybersecurity-laws-june-2022/#:~:text=U.S.%20Passes%20New%20Cybersecurity%20Legislation%20in%20June%202022&text=The%20State%20and%20Local%20Government,%2C%20tribal%2C%20and%20territorial%20governments. (last visited Dec 24, 2021, 12:55 P.M.)
[39] People's Union of Civil Liberties v. Union of India and Anr. AIR 1997 SC 568

mechanisms. The Indian Parliament passed the ''Information Technology Act, 2000[40],'' in order to formulate strict statutory laws to regulate the criminal activities in the cyber world to protect the fields of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cyber-crimes. The Act was further amended in the form of Information Technology Amendment Act, 2008.[41]

Lack of privacy in Cyberspace

With the technological development, there need to be amendment in the cyber laws too.

- The continuing advancement of cyberspace, as a fully electronic world created by interrelated networks in parallel with our physical environment, is characterized by an enormous amount of data.

- Suppose, in online banking, social networking or other services, one may risk a theft to your personal information such as name, address, credit card number etc. Unscrupulous people can access this information through unsecured connections or by planting software and then use your personal details for their benefit.

- When any virus attacks Internet then, users are often plagued by virus attacks on their systems. One may get activated this virus attacks if one clicks any link. Computers connected to the Internet are very prone to targeted virus attacks and may end up crashing.

- When one is blindly pursuing compliance may actually put an organization at increased risk specifically because it is focused on a "check-the-box" compliance model leading to a false sense of security, whereas performing proper risk management requires organizations to scour and identify areas where additional safeguards are needed.

- Unfortunately, the ability to send and receive emails also created a means for cybercriminals to distribute spam and malware. Malware hiding in email attachments could wreak havoc to your PC or possibly even create a backdoor for an attacker to infiltrate your

[40] The Information Technology Act, 2000 (09 of 2000) Acts of Parliament, 2000 (India)
[41] Ibid 40.

system. Through email, cybercriminals saw this as another opportunity to play on human emotions and lure victims into revealing sensitive information through phishing scams.

Thus, to combat these above problems at that very time or to take appropriate actions cyber laws must be eligible and potent to handle all cybercrimes and protect internet users from any harm.

Conclusion

Nations are constantly trying to combat the new age cybercrimes by amending the existing laws. Internet usage is so intertwined with every aspect of human life that it has become inseparable. Therefore, cyber laws have to be potent to protect individuals from any cybercrimes.

In my opinion cyber laws in India needs to be more effective when it is compared to that of USA. USA has their laws from 1980s and in India the cyber laws were just developed in 2000. Indian cyber laws later amended in 2008 and came to be known as Information Technology Act, 2008. Just as Article 21of the Indian Constitution depicts right to privacy of any citizen of India, therefore the Information Technology Act, talks about right to privacy in cyber space and combat other crimes too like hacking, Cyber Stalking, Cyber Pornography, etc.

USA is the cradle of technology so laws pertaining to the combat of cybercrimes are very efficient in the nation. Various Acts like Cybersecurity Information Sharing Act, National Cybersecurity Protection Advancement Act of 2015, etc.

With advancement of time, India should regulate its cyber laws and there should be efficacy in implementing not only the Information Technology laws but also the Evidence Act and the Indian Penal Code when any internet user has fall prey to any cybercrimes. The Digital Personal Data Protection Act, 2023 has served the purposes to the extent. There should be exemplary punishments so that any person should think twice to commit any harm to any individual in cyber space and effective remedies to the internet users falling prey to any cybercrime.