SHODH SAMAGAM

ISSN : 2581-6918 (Online), 2582-1792 (PRINT)

The Future of Digital Privacy and Cyberstalking: A Legal Viewpoint

Narendra Kumar Thapak, Ph.D., School of Legal Studies & Vice Chancellor
Udit Agnihotri, Research Scholar, School of Legal Studies
LNCT University, Bhopal, Madhya Pradesh, INDIA

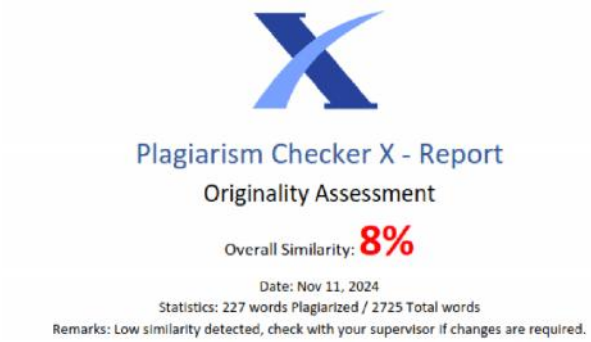
ORIGINAL ARTICLE

Authors

Narendra Kumar Thapak, Ph.D.
Udit Agnihotri, Research Scholar
E-mail : Nkthapak@gmail.com

shodhsamagam1@gmail.com

Received on : 09/09/2024
Revised on : 09/11/2024
Accepted on : 19/11/2024
Overall Similarity : 08% on 11/11/2024



ABSTRACT

A 2018 study by the National Crime Records Bureau (NCRB) found that stalking incidents occur in India at least once every fifty-five minutes. Offenders have a great potential to misuse cyber technology, even while this widespread cyber development opens up new avenues for knowledge acquisition. As the number of internet users rises, stalking has also become more common in the online community, where it is now referred to as "cyberstalking," "e-stalking," or "online stalking." In addition, a number of software programs, such as spyware and stalk ware, are now readily accessible and can be used to misuse technology and carry out covert monitoring without a person's knowledge or agreement. It is noteworthy that a recent study discovered that the crime of cyberstalking increased significantly during the 2020 COVID-19 shutdown period.

KEY WORDS

Data Protection, Cyberbullying, Online Harassment, Cyberstalking, United Kingdom, India.

INTRODUCTION

The term "Star-Stalking" refers to stalking behaviours that were more focused on celebrities by their fans in the early 1990s.[1] Criminal activity has spread to the virtual world these days, and it is no longer exclusive to the physical world. The everyday routines of human life have undergone remarkable transformations as a result of cyberspace in this digital age. Originally developed for the benefit of society and to improve people's comfort and lifestyle, information and communication technology has progressively evolved into a tool for criminal ambitions.[2] The three as of cyberspace anonymity, authority, and attention not only draw criminals but also give regular

individuals a chance to indulge their darker side and have fun.[3]

These stalkers typically want to get inside their target's personal space. By the form of persistent emails, texts, obnoxious phone calls, or any other method, cyberstalkers attempt to track their target's every action. However, the right to privacy being an international human right has been well recognized by the Universal Declaration of Human Rights [4] since 1948 as well as under the International Covenant on Civil and Political Rights [5] since 1966. The Indian Supreme Court has since unequivocally confirmed that the right to privacy is an essential component of the fundamental rights protected by Article 21 of the Indian Constitution.[6] "Just because a person is in a public setting does not indicate a loss or surrender of private," the Supreme Court noted in this context. One essential component of a person's personal dignity is their right to privacy. Therefore, in addition to causing the victim to feel threatened and grieved, this cyberstalking behaviour also breaches their fundamental human rights to privacy, dignity, and personal liberty.

Cyberstalking is the practice of stalking or harassing a person, group, or organization over the internet or other technological methods. AI developments have made this problem worse by making cyberstalking tactics more complex. By automating and improving stalking activities, artificial intelligence (AI) can help offenders obtain personal data, monitor movements, and even forecast behaviour. Because of this, safeguarding people's digital privacy has become more difficult. Protecting personal data and information from misuse and unwanted access is known as digital privacy. Because AI systems can handle large volumes of data rapidly and efficiently, which could result in privacy breaches, the rise of AI has made efforts to protect digital privacy more difficult. AI-powered solutions are able to monitor digital.

While the current legal framework in India covers some aspects of digital privacy and cyberstalking, it might not be sufficient to handle the issues raised by artificial intelligence. Section 354D of the Indian Penal Code (IPC), for example, makes repeated attempts to contact or monitor someone without that person's consent illegal. This section explicitly targets stalking, including cyberstalking. [7]Furthermore, the Information Technology (IT) Act, 2000, has clauses that penalize the dissemination or publication of pornographic material as well as violations of privacy and confidentiality.[8] To better protect people's rights in a world that is becoming more digital, adjustments may be necessary, nevertheless, given the speed at which AI is developing and the intricacy of cybercrimes. This could entail improving enforcement procedures, raising awareness and educating people about digital privacy and cyberstalking, and revising current legislation to address emerging AI-driven risks. It is evident from analysing the relationship between artificial intelligence, cyberstalking, and digital privacy in the framework of Indian law that, despite advancements, much more has to be done to guarantee that people's rights are sufficiently safeguarded in the digital era.

In the framework of Indian law, this Article examines the relationship between artificial intelligence, cyberstalking, and digital privacy. It looks at the existing legal system, how well it handles these issues, and whether any changes are necessary to protect people's rights in a world that is becoming more and more digital.

The Legal Situation in Other Nations

Instead of having particular laws to prevent cyberstalking, most countries use general laws (as applicable in cases of blackmail, extortion, threats, defamation, outrage of modesty, harassment, theft, invasion of privacy, online impersonation, hacking, etc.) to prosecute cyberstalkers.[9] However, the following analysis only considers the position of industrialized nations like the United States and the United Kingdom:

I. **Status of the Law in the United States:** Section 2261-A sub-section 1 of Title 18, United States Code (U.S.C.), a federal statute of the United States of America (USA), addresses traditional stalking, whereas Section 2261-b expressly makes "cyberstalking" a crime. Cyberstalking violators face a maximum penalty of 20 years in jail, a maximum penalty of 10 years, a maximum penalty of 5 years, or a fine based on the victim's injuries under Section 2261-b. Other rules, such as those pertaining to

threats and extortion, may also be relevant against cyberstalkers in addition to this specific clause for "cyberstalking."[10], offensive or persistent phone calls[11], creation of child pornography, luring or pressuring a youngster, hacking into a computer, etc. Moreover, the recent issue of cyberstalking prompted an amendment to the Federal Telephone Harassment Statute, 1934, in 2006. A broader definition of telecommunication devices now includes any software or device that uses the internet for communication. Additionally, it imposes a two-year jail sentence for using a telecommunications device that annoys, abuses, or threatens someone.[12]

In the United States, cyberstalking is subject to a civil remedy. In the US, there is a civil remedy for cyberstalking. Therefore, in addition to whatever other incidental restrictions the court determines are appropriate, a civil injunction order prohibits the stalker from getting in touch with you ever again. The court may also bring a contempt of court proceeding against the offender if a violation occurs. As a result, a civil injunction order forbids the stalker from contacting you again, as well as any other incidental orders the court deems appropriate. If a violation does place, the court may also file a contempt of court case against the offender.[13]

The U.S. Department of Justice has issued guidelines that advise victims of cyberstalking to save any emails, messages, and other correspondence as evidence to help prosecute the perpetrator. The actual electronic copies, not simply printouts, must be kept at the source and cannot be altered in any manner. Additionally, it requires Internet service providers (ISPs) and Government enforcement to maintain detailed records of all communications. It is important to keep track of every report you submit to any agency or provider and to get copies of the official reports when you need them.[14]

II. **Laws in the United Kingdom:** In the UK, there is not any special rule against cyberstalking; instead, there are a few general statutes that combat the crime. These are (I) The Protection from Harassment Act,[15] 1997 (ii) The Malicious Communications Act,[16]1988 (iii) The Computer Misuse Act,[17] 1990 (iv)The Crime and Disorder Act,[18] 1998 (v) The Communication Act,[19] 2003; (vi) The Serious Crimes Act,[20] 2007; (vii) The Criminal Justice and Courts Act[21], 2015 in addition to a number of other laws. The following is an enumeration of the few most pertinent provisions:

The Protection of Freedoms Act of 2012 revised the Protection from Harassment Act of 1997, adding two new stalking-specific provisions (sections 2A and 4A), which may also apply to cyberstalking. Although the terms "stalking" and "cyberstalking" are not defined explicitly, Section 2A (3) lists specific actions or inactions that would qualify as stalking and stipulates that offender faces a maximum 51-week jail sentence, a level 5 fine, or both if found guilty in summary. In addition to providing suitable penalties, Section 1 of the Malicious Communications Act of 1988 prohibits sending any letter, electronic message, or material that is offensive, threatening, or indecent and that causes distress or worry.[22]

An Analysis of Indian Laws Pertaining to Privacy Protection in Cyberspace

Seldom does privacy itself entail making an effort to hide one's behaviour from the general public. Simply put, privacy is the demand that rules pertaining to individual accountability and public security not encroach on one's personal opinions and behaviours that are irrelevant to the general public. Determining the boundaries of "privacy" is difficult. The phrase "the right to be left alone" was also coined by Warren and Brand in their landmark law review article from almost a century ago. Personal autonomy, which encompasses the different libertarian schools that also connect freedom with personal sovereignty, is another term for privacy. "The life of the law has not been logic: it has been feeling," as Oliver Wendell Holmes once stated.[23] Privacy was a theme that had great appeal to Louis Brandeis. In an often-quoted dissent in Olmstead v. the United States (1928)[24], the significance of which was later recognized, Justice Brandeis wrote:

"Our Constitution's framers committed to creating an environment that is conducive to pursuing happiness. They granted, as opposed to the Government, the right to be granted, let alone the most

extensive of rights and the right most prized by civilized men, since they understood the importance of man's spiritual nature, sentiments, and intellect.

India lacks a distinct law that is only focused on data protection, in contrast to the European Union. In the context of the "Right to Privacy" implied in Articles 19 and 21 of the Indian Constitution, courts have, however, on multiple occasions construed "data protection" within these parameters. BN Srikrishna, a former Supreme Court judge, is leading an expert panel that the Ministry of Electronics and Information Technology has established to create a data protection law.

This right outside of one's house is not absolute, just as the right to privacy is not absolute even within one's own home. Naturally, one's expectation of privacy decreases as they go from a private to a more public sphere. In fact, the courts have placed a great deal of stress on striking a balance between the right to privacy and other rights when attempting to apply the latter.

The Information Technology Act, 2000 as Amended in 2008: Relevant Provisions

The Information Technology Act was enacted in 2000 and has been revised most recently 2008. The Information Technology (Amendment) Act, 2008 has added several provisions that are privacy-centric. Sections 43 deals with Penalty and Compensation for damage to computer, computer system, Section 66 deals with computer related offences, Section 66-C deals with Identity Theft or Hacking, Section 66 D provides punishment for Cheating by Personation by using computer source, Section 66 E deals with punishment for violation of privacy, Section 67 C provides Preservation and Retention of information by intermediaries, Section 69 states powers to issue directions for interception or monitoring or decryption of any information through any computer resource, Section 72 mentions regarding privacy and confidentiality and Section 72 A deals with Punishment for Disclosure of information in breach of lawful contract (Inserted vide ITAA-2008) of the Information Technology Act, 2000, which relate to computer/cybercrimes. The Act is lacking in many ways, including: (1) No definition of "sensitive personal data" is clearly defined. (2) The IT Act is silent on Cyber privacy issues. (3) The IT Act makes hacking and tampering with computer source an offence and penalizes unlawful access to data. However, does not prescribe any minimum-security standards which the entities having control of data should comply with except in cases of Personal sensitive information.

The Data (Privacy and Protection) Bill 2017 & 2019

The purpose of the Justice BN Shrikrishna Committee was to examine current concerns and potential legal safeguards while putting forward a draft data privacy framework. There is a statutory right to privacy under the Data (Privacy and Protection) Bills of 2017 and 2019. By offering a comprehensive framework and suggesting the establishment of the Data Privacy Act, the Bill also seeks to simplify India's data protection laws. This Bill has addressed a number of new privacy concerns, including "reasonable expectations," internet banking, "due diligence," "consent criterion," BHIM (Bharat Interface for Money), and others. The purpose of the Justice BN Shrikrishna Committee was to examine current concerns and potential legal safeguards while putting forward a draft data privacy framework. There is a statutory right to privacy under the Data (Privacy and Protection) Bills of 2017 and 2019. By offering a comprehensive framework and suggesting the establishment of the Data Privacy Act, the Bill also seeks to simplify India's data protection laws. This Bill has addressed a number of new privacy concerns, including "reasonable expectations," internet banking, "due diligence," "consent criterion," BHIM (Bharat Interface for Money), and others.

Strengthening the Personal Data Protection Bill

The PDP Bill, once enacted, will play a crucial role in protecting digital privacy in India. However, it must be strengthened to address AI-specific concerns, such as the use of AI in data processing and the potential for AI-driven privacy violations. The Bill should include provisions for the ethical use of AI, transparency in AI decision-making, and accountability for AI-driven actions. The Personal Data Protection Bill (now the Digital Personal Data Protection Act, 2023) aims to create a comprehensive framework for the protection

and processing of personal data in India. Its primary objectives are ensuring that individuals' personal data is safeguarded against misuse and unauthorized access, Striking a balance between an individual's right to privacy and the necessity of processing personal data for legitimate purposes, Mandating that organizations be transparent about their data processing activities and hold them accountable for any misuse or breaches, Empowering individuals by giving them more control over their personal data, including the right to consent to data processing and the ability to withdraw consent and establishing clear legal guidelines and standards for data protection, ensuring compliance with global data protection norms.

CONCLUSION

According to a vast number of criminologists, laws and regulations that apply to traditional stalking will not be adequate to address cyberstalking. Similarly, while section 354-D of the IPC may cover cyberstalking, it has little bearing on defending an individual's inherent right to privacy. However, section 66-A of the IT Act only addressed a handful of the behaviours associated with cyberstalking; it was not a complete regulation. The Supreme Court finally overturned it in 2015 for violating the right to free speech and expression guaranteed by the constitution. But in 2017, the Supreme Court ruled that the right to privacy is an essential component of the right to life and personal freedom. Furthermore, cyberstalking must be protected since it infringes on an individual's right to privacy and is not a minor offense that can be limited in the context of freedom of speech and expression. It is meaningless to point out that Article 19 itself places limitations on the right to free speech and expression, and that these limitations should not lead to a breach of an individual's right to privacy. Additionally, no law has attempted to eliminate the potential of privacy violations brought on by cyberstalking. Many cyberstalkers might feel free to commit this kind of cybercrime even if there are no laws specifically prohibiting it. Therefore, it is necessary to include a provision for cyberstalking while taking into account the risk to one's right to privacy.

In conclusion, the future of digital privacy in India will depend on the ability of lawmakers, courts, and society to adapt to the rapidly changing technological landscape. By addressing the challenges posed by AI, India can create a legal framework that not only protects individuals from cyber stalking but also ensures that digital privacy remains a fundamental right in the age of artificial intelligence.

REFERENCES

1. Joel Best, Stalking, Encyclopaedia Britannica, June 6, 2016 available at: www.britannica.com/topic/stalking crime/cyberstalking accessed, Accessed on 13/08/2024.
2. Ehsan Salimi & Abbas Mansour Abadi (2014) The Criminology of Cyber Stalking: Investigating the Crime, Offenders and Victims of Cyber Stalking, *International Journal of Criminology and Sociological Theory* 7(2) .
3. Merriam-Webster Legal Dictionary, Cyberstalking, available at: www.merriam-webster.com/legal/cyberstalking, Accessed on 07/09/2024.
4. Universal Declarations of Human Rights, G.A. Res. 217A, U.N. Doc. A/810 (December 12, 1948), Art. 12: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.
5. International Covenant on Civil and Political Rights, G. A. Res. 2200A (XXI) (December 16, 1966), Art. 17.
6. Justice K. S. Puttaswamy (Retd.) & Ors v. Union of India & Ors. (2017) 10 SCC 1; AIR 2017 SC 4161.

7. Laws Punishing Cyber Stalking and Online Harassment https://blog.ipleaders.in/cyber-stalking, Accessed on 22/08/2024.
8. What Are the Laws on Cyber stalking in India? https://blog.ipleaders.in/cyber-stalking, Accessed on 22/08/2024.
9. United Nations Office on Drugs and Crime, Cyberstalking and Cyber harassment, May 2019, available at: www.unodc.org/e4j/en/cybercrime/module-12/key-issues/cyberstalking-and-cyberharassment.html., Accessed on 07/09/2024.
10. 18 United States Code § 875, 876 (U.S.).
11. 47 United States Code § 223 (U.S.).
12. Naomi, Harlin Goodno (2007) Cyberstalking a New Crime: Evaluating Effectiveness of Current State and Federal Laws, 72 Missouri Law Review, 146.
13. Joey L. Blanch & Wesley L. Hsu (2016) An Introduction to Violent Crime on the Internet, *United States Attorneys' Bulletin 2*, 64(3).
14. Alexis A. Moore, 12 Tips to Protect Yourself from Cyberstalking, Thought Co., January 8, 2009, available at: www.thoughtco.com/tips-toprotect-yourself-from-cyberstalking-3534318, Accessed on 07/09/2024.
15. Protection from Harassment Act, 1997 (c 40) § 2A and 4A (U.K.).
16. Malicious Communications Act, 1988 (c 27) § 1 (U.K.).
17. The Computer Misuse Act, 1990 (c 18) § 1 (U.K.).
18. The Crime and Disorder Act, 1998 (c 37) § 32 (U.K.).
19. Communications Act, 2003 (c 21) § 127 (U.K.).
20. The Serious Crimes Act, 2007 (c 27) § 44-46 (U.K.).
21. The Criminal Justice and Courts Act, 2015 (c 2) § 33-35 and Sch. 8 (U.K.).
22. The Protection from Harassment Act 1997 (c 40) § 2A (4) (U.K.).
23. In 1890, Louis Brandeis, and his law partner Samuel Warren (1928) wrote the most famous article on the right to privacy in American history. Warren and his young wife, Mabel, were upset about gossip items in the Boston society press including stories about Mrs. Warren's friendship with President Grover Cleveland's young bride and this aristocratic distaste for invasions of what Warren called their "social privacy" led him to seek Brandeis's help in proposing a new legal remedy. https://www.washingtonpost.com/opinions/clash-between-free-speech-and-privacyin-the-digital-world/2015/03/20/bee390e6-c0f8-11e4-ad5c-3b8ce89f1b89_story.html?utm_term=.b26b05f931c5, 24 277 U.S. 438, Accessed on 05/09/2024.

****