Lucknow Law Review

Long Article

Cyber Stalking: A Socio-Legal Study

Munira Bharmal[1]

[1] *United World School of Law, Karnavati University, Gandhinagar*

Published on: February 27, 2022
Page No.: 65 – 77
Manuscript No.: 2022/LWLR/27065
Editors: Saman Rahman, Deepayan Malaviya

Cite as: Munira Bharmal, Cyber Stalking: A Socio-Legal Study (2022) 1(3) LKO. L. REV. 65

Find here: *https://www.lucknowlawreview.org/munira-bharmal*

Abstract: *In their employment, education, and social lives, people utilize the internet to communicate locally or globally. As the number of people using the internet has grown, so has the number of incidences of online harassment and cyberstalking. To put it another way, the internet era has opened up a world of previously unknown criminal opportunities that defy and go beyond all physical boundaries, countries' borders, and limits in the pursuit of detecting, punishing and alleviating what appears to be a global problem. As a result of the internet a new sort of criminal has emerged known as the cyber stalker – a criminal who employs advanced stalking methods to prey on, harass, threaten, and create enormous dread and terror in their victims using the internet as a tool or weapon. Cyberstalking is one of those crimes that has been increasingly popular in recent years as low-cost, high-speed internet access has become more generally available. Because no tangible evidence is necessary and no witnesses are required for conviction, cyberstalking is far more accessible than other offenses. It's a term that mainly refers to obtaining personal information from someone else to commit fraud or identity theft. It can involve impersonating another person, gaining financial or personal information from them, and then using that information without their permission. This has become a typical occurrence in recent years, with several cyber-threats occurring on a yearly basis. This article delves deeper into this topic with a socio-legal analysis of Indian and UK legislation, as well as legislation aimed solely at online conduct, and discusses the weaknesses in these laws.*

Keywords: *Stalking, Cyber, IT, Penal.*

1. Introduction

Computers and communications reflect today's rapidly changing, high-tech environment. Cyberspace is an environment that is continually evolving, undefined, and exponential. People who use the internet have increased dramatically as a result of the Information Technology (IT) revolution. It's changed the game in every field possible, including business, education, sports, and entertainment.

The internet, on the other hand, has negatives impact, such as the rise of new and different sorts of crimes, such as online-based illicit operations. In general, these are referred to as "cybercrimes". Such activities have the same impact on our private, economic, and social life as physical crimes, and they are just as distressing and hurtful. Some academics have made the strange claim that "nobody knows you're a dog on the Internet".[1] In recent years, computer crimes, sometimes known as cybercrimes, have risen significantly, with cyberstalking being one of the most hazardous. Cyberbullying is a pattern of threatening or malevolent conduct that involves the usage of the Internet, mail, or other digital language communication to personalize an individual.[2]

2. What is Cyberstalking

Cyberstalking is a criminal legal term that refers to:

1. Monitoring and collecting information about an individual using the internet.
2. Using such information for malicious purposes.
3. Violently attacking or threatening an individual.

Cyberstalking can be used to harass someone, but it is often difficult to prove that cyberstalking took place and will not necessarily result in criminal charges. Cyberstalking is an act that can be committed through the internet, mobile phones, or other electronic devices. Cyberstalking is frequently associated with online harassment, using software to monitor an individual's activities. Cyberstalking may also occur in person, but typically *via* email or social networking sites like Facebook, Instagram, and Twitter. Cyberstalking can be a form of cybercrime and a form of cyberbullying, which is frequently perpetrated by perpetrators that are teenagers or pre-teenagers.

[1] Christopher Reed, *Internet Law: Text and Materials* (Cambridge 2000) 119
[2] Michigan Criminal Defense, 'Cyber Stalking and Cyber Harassment Charges in Detail' (*Not Afraid to Win*, 10 February 2020) <https://www.notafraidtowin.com/cyberstalking-cyberharassment/> accessed on 10 November 2021

Cyberstalking, also referred to in this paper as online stalking, can be compared to physical stalking, which is becoming more prevalent as a result of modern technology. Cyberstalking has the identical characteristics as conventional stalking, but it is fundamentally altered when it is translated into the virtual realm. Cyberstalking is a new method of stalking that involves the usage of the internet or any sorts of digital communication. Cyberstalking is a digital "assault" on a single person who has been singled out for revenge, power, or anger. Some examples of cyberstalking are as follows:

1. Victim humiliation, embarrassment, and harassment,
2. using other types of monetary control, such like destroying the victim's credit score, emptying bank account, or impose other forms of economic control,
3. isolating the victim by harassing family, friends, and co-workers,
4. fear-instilling scare tactics, among other things.

In general, cyberstalking is a pattern of behaviour that occurs over time and comprises repeated purposeful attempts to disturb the victim. It consists of a way of conduct that would make a reasonable person fearful. Attempts to agitate the sufferer on a regular basis. It's characterised as a pattern of behaviour that would frighten a rational person. The stalker's systematic, premeditated, and persistent attempts, which continues beside the victim has requested the stalker to cease associating with them, constitute cyberstalking. The victim's daily routine is entirely disrupted, and their mental health is harmed. Stalkers may now openly broadcast statements about the victim thanks to the emergence of social media, allowing them to torment the victim in front of a virtual wider crowd. It may also have an impact on the victim's work life, as she will be unable to use the internet for a period of time in order to stop the unwanted communication.

3. Understanding the Legislative Framework in India

In India, the legislations do not directly address cyberstalking. However, this offence is linked to the some of the provisions of the Indian Penal Code[3] and the Information Technology Act[4], which has been clarified. Let's look at the Indian rules on cyberstalking in more detail:

[3] Indian Penal Code 1860
[4] Information Technology Act 2000

1. Section 354D of the Indian Penal Code[5]

1) Any male who:

(i) pursues a woman and regularly contacts or wants to contact her in order to foster an intimate relationship, notwithstanding her obvious aversion; or,
(ii) monitors a woman through internet, electronic-mail, or any other electronic communication.

Provided, however, that the person who pursued it can show that:

(i) it was pursued to prevent or discover the crime, and the State had entrusted the individual accused of stalking with the task of preventing and detecting crime; or,
(ii) it was pursued to comply with any law or any condition or obligation imposed by anyone under any law; or,
(iii) it was appropriate and justified given the circumstances.

In reaction to a gang-rape case in Delhi, the clause was introduced to the Criminal Amendment Act, 2013. According to the Section, any person who tries to track the online activities of a woman, is accused of cyberstalking. As a result, the stalker might be charged below Section 354D of the Indian Penal Code if he commits any of the offences specified there.

This Section has various faults, certainly considered one among that's that it simplest recognizes "women" as victims, ignoring the reality that man also can be victims. In accordance with the Section, any person who seeks to traces a woman's usage of the internet activity, e-mail, or any other kind of verbal digital communication is accountable for cyberstalking. It is evident that it is primarily directed at women. As a result, the law is skewed in favour of women. Furthermore, the lawmakers have not specified the "means of monitoring". Although it`s possible that the man had no purpose of stalking, even though his action were amounts to stalking.

The provision is also silent on whether or not an offending post or message should be removed from the internet, and it disregards the victim's emotional and psychological distress. The proviso to Section 354D now excludes some activities from the meaning of stalking. These exclusions are based on Section 1(3) of the United Kingdom (UK) harassment legislation, the Protection from Harassment Act, 1997. However, it is uncertain if the exception's broad phrasing, particularly the last section, which allows for the invasion of

[5] Indian Penal Code 1860, sec. 354D

privacy and confidentiality if the conduct is fair and justified in the circumstances, will withstand constitutional scrutiny.

This Section contains an ambiguity issue, allowing law enforcement officials to breach a person's privacy at will. This sentence appears to go against the judgement in the historic case of *PUCL* v. *Union of India*[6], in which the Apex Court set norms to govern the state's jurisdiction under Section 5 of the Telegraph Act[7]. It was determined by the court that wiretapping breaches the right to privacy, and that the authority conferred beneath Section 5 can only be employed in the situation of a national emergency or when security of a public at large is at risk. However, in such case, the regulations must be observed.

There's no cause why these procedural precautions shouldn't apply to online interactions, and doing so would be a violation of the ruling's norm. According to the first proviso, someone entrusted with the State's responsibility for crime prevention may engage in online stalking. According to the first proviso, a man charged with the State's responsibility for crime prevention may also engage in cyberstalking to prevent or detect a crime.

In *Kharak Singh* v. *State of Uttar Pradesh*[8], The Supreme Court held that Section 236 of the Uttar Pradesh Police Regulations[9], which permitted domiciliary visits, was unconstitutional since it is in infringement of Article 21 of the Constitution. Quoting Frankfurt J., from *Wolf* v. *Colorado*[10], the court decided that police intervention into a person's home sanctity and security infringes Article 21 – 'right to personal liberty'.

2. Section 292 of the Indian Penal Code[11]

This Section of the Indian Penal Code defines 'Obscenity' which means sending of obscene content *via* a social networking site, email, text message, or other means to a victim. It falls under the category of cyberstalking. Suppose stalker tries to annoy the victim by means of sending obscene material over the Internet for them to read, view, or hear. Then the person is in violation of Section 292 of the Indian Penal Code in this case.

[6] *PUCL v Union of India* AIR 1997 SC 568
[7] Telegraph Act 1885, sec. 5
[8] *Kharak Singh v State of Uttar Pradesh* 1964 SCR (1) 332
[9] Uttar Pradesh Police Regulations 1861, sec. 236
[10] *Wolf v Colorado* 338 U.S 25 (1949)
[11] Indian Penal Code 1860, sec. 292

3. Section 507 of the Indian Penal Code[12]

This Section of Indian Penal Code covers anonymous communication as a means of "criminal intimidation". The Section indicates that concealing the stalker's identity in order for the victim to remain unaware of the danger's source is penalised. As a result, it ensures obscurity, which is crucial in cyberstalking. This provision makes a stalker guilty if they try to hide their identity.

4. Section 509 of the Indian Penal Code[13]

This Section deals with women's modesty – "a word, gesture, or action meant to offend a woman's modesty — Whoever, with the intent of insulting a woman's modesty, utters any phrase, makes any sound or motion, or shows any item with the intent that such word, sound, gesture, or object be heard, or that such gesture or object be seen, by such woman, or intrudes upon her solitude, must be penalised".

This provision may apply if a stalker makes obscene gestures or communicates filthy statements to a lady *via* e-mail, texting, or social media. If he performed any of these actions, he would be charged under Section 509 of the Indian Penal Code.

Section 509 contains a number of faults. One of those is a gender-prejudice clause that emphasises on the modesty of a woman at the same time as ignoring the fact that cyberstalking, a gender-impartial offence, can affect each woman and man equally. In this Section, the words, voice, or gesture ought to be spoken, heard, and visible withinside the order listed. Cyber-stalkers can undoubtedly run-away the sanctions imposed by this rule because words ought to be uttered, gestures cannot be observed, and sound cannot be heard through the internet.[14] Finally, one cannot infer an intent to violate a woman's modesty from internet comments.

5. Section 67A of the Information Technology Act[15]

This Section addresses one component of cyberstalking. After a revision in 2008, this Section was introduced. It specifies that stalkers who seek to electronically transmit "sexually explicit" information *via* email, text message, or social media shall be punished and penalized under Section 67A of the Information Technology Act.

---

[12] Indian Penal Code 1860, sec. 507
[13] Indian Penal Code 1860, sec. 509
[14] Pawan Duggal, 'The Scary Reality of Cyberstalking: The Law Can't Protect Us (Yet)' (*The Quint*, 13 May 2017) <https://www.thequint.com/voices/opinion/the-dark-world-of-cyberstalking-and-how-the-law-cant-protect-us>
[15] Information Technology Act 2000, sec. 67A

6. Section 67B of the Information Technology Act[16]

This Section is a new inclusion by the Amendment Act of 2008. The Section concentrates on stalkers who focuses on juveniles below the age of 18 and terrorise them by distributing films of children engaging in sexual acts.

7. Sections 66E of the Information Technology Act[17] read with 354C of the Indian Penal Code[18]

The Sections encompass "voyeurism". According to Section 66E – "whoever, willfully or knowingly obtains, captures, publishes, or transmits a photograph of a person's private area without their consent, under circumstances that violate that person's privacy, will be penalised."

The following is the text of Section 354C - "any man who watches or captures the picture of a woman participating in a private act under circumstances where she would normally expect to be unobserved, either by the perpetrator or by any other person acting on the perpetrator's behalf, and then disseminates such image is guilty shall be punished".[19]

Using personal images on social networking platforms to cause misery and fear in the victim's psyche. Both legislations seek to make it illegal to publish or photograph someone's private life absent their permission. Section 66E, on the opposite hand, is greater inclusive due to the fact the victim is noted as "any individual", while Section 345C is greater gendered. The victim ought to be a "woman", consistent with 354C. While all offline regulations apply to virtual media, the Information Technology Act imposes a ways harsher penalty.[20] In essence, the Women's bodies and sexualities are given a lot of attention in the Information Technology Act, under the Section 66A addressing a wide range of "offensive comments".[21]

The Information Technology Act of 2000 and the Indian Penal Code of 1860 does not directly get to grips with cyber stalking or the stalker's defamatory or threatening statements made while stalking the victim *via* text, tele cellphone calls, electronic mails, and a blog using the victim's name.

16 Information Technology Act 2000, sec. 67B
17 Information Technology Act 2000, sec. 66E
18 Indian Penal Code 1860, sec. 354C
19 Indian Penal Code 1860
20 Richa Kaul Padte, 'Keeping Woman Safe? Gender, Online Harassment and Indian Law' (2013) 48(26-27) EPW
21 *Ibid*

Although any Section of the aforementioned legislation can be utilized to punish the offender, there is no formal act that particularly addresses this criminal act. Thus, such crimes are easy to commit, but the consequences are serious. This can harm the emotional and physical well-being of the victim.

4. Legislative Framework in United Kingdom

There is no specific regulation dealing with online stalking in the United Kingdom. Instead, three important legislations are used to combat harassment, also used in stalking situations. The Telecommunications Act of 1984, the Protection from Harassment Act of 1997, and the Malicious Communications Act of 1988 are the three primary laws used to deter stalking and cyberstalking. According to the Telecommunications Act of 1984, it is prohibited to transmit inappropriate, threatening, or profane communication. People who send letters or distribute publications with the intent of causing fear or terror in others are punished under the 1988 Act, which has a broader reach.

The Protection from Harassment Act of 1997 was primarily enacted as a bill to prevent stalking, but it was always intended to cover all types of abuse, including stalking. Even though stalking offences were punished under the Protection from Harassment Act of 1997, many stalking victims thought that the criminal justice system did not take them seriously and that stalking should be a significant felony.

The Section 111 of Protection of Freedoms Act[22], introduced the following two crimes to the Protection from Harassment Act, and following are some examples of new stalking offences:

- Stalking is a distinct behaviour, as opposed to harassment in general.
- The gap has been narrowed when a set of behaviours did not create fear of violence in victims but still caused severe concern or distress. In this case, the police and public prosecutors may consider only summary crimes under Article 2.
- New Section 4A crimes include an additional element that can be prosecuted even if the defendant's actions do not indicate a fear of violence.
- Acts as a protective barrier for victims of persecution.

According to Section 1 of the Protection from Harassment Act 1997, "A person shall not engage in any conduct that harasses another person, nor shall he engage in any activity that he/she should know or should be aware of." According to Section 2A of this law, persecution requires three conditions: 1) act of the offender,

[22] Protection of Freedoms Act 2012, sec. 111

2) act violates Section 1 of the Act, 3) acts amounts to stalking. Although stalking is not legally defined, Section 2A (3) of the Protection from Harassment Act offers a variety of instances of stalker behaviours:

- following someone,
- contacting or attempting to contact someone,
- Surveillance of a person's internet or electronic communication usage,
- Monitoring a person's internet or electronic communication usage,
- spying on or observing another individual,
- tampering with another person's property,

The list in Section 2A (3) is not complete, and courts may decide that other activities by a defendant constitute stalking even if they are not on the list. The defence is likely to claim that some "stalking-related" conduct should be classified as harassment rather than stalking and that the accused is guilty of harassment rather than stalking. When such an argument is offered, it is a factual choice for the magistrates to make. As a result, it's crucial to start with the proper charge. The offence of stalking is a summary offence under Section 2A, and anybody who commits it faces serious consequences. Section 2A is a summary offence, and anybody found guilty of stalking faces a maximum penalty of six months' imprisonment or a fine if convicted on summary conviction. Section 2A crime, being a summary only offence, necessitates filing a piece of information or complaint within six months of the time the offence was committed, or the issue of criticism arose. The six-month period shall begin on the final day of the claimed course of action.

4.1. Stalking: Section 2A

If the suspect can establish that any of the harassment defences under Section 1(3) of the Protection from Harassment Act are valid, they cannot be found guilty of stalking since stalking is hard to prove without harassment.

4.2. Putting People in Fear of Violence: Section 4A (1)(b)(i)

The components of a Section 4 (1)(b)(i) offence are:

- a series of behaviour,
- that leads someone to fear that violence will be used against him; and.
- which is something the accused knows or should know will cause another to dread initiating violence towards him; and,

- The defendant should be aware that his actions would cause another to fear that violence will be used against them if a reasonable person in the same situation would believe that the defendant's actions would lead the other to fear that violence would be used against them on that situation.

The following legislative shields are also included in Section 4. The defendant must prove that:

- the series of behaviour was pursued the purpose of preventing or detecting crime;
- the series of behaviour was pursued under any enactment or the rule of law, or to comply with any condition or requirement imposed by any person under any legislation; or
- The series of behaviour was pursued for the protection of him or herself or another, or for the protection of her, his or another's property.

The components of the section 4A offence are:

- a series of behaviour,
- which results in stalking; and,
- that leads someone to fear that violence will be used against him in two situations; or,
- creates another severe alarm or anxiety that has a significant negative impact on their normal day-to-day activities.

The question to be assessed is whether a reasonable person in possession of the same facts would believe the defendant should know that his or her actions will cause the other person to fear that violence will be used against them or will cause the other person considerable worry or distress. A series of behaviour is the same as the definition given in Section 7 of the Protection from Harassment Act 1997, mentioned previously in the guideline. This offence can be committed in two ways:

- First, a pattern of behaviour that amounts to stalking and makes the victim believe that violence will be used against them in at least two situations which is similar to the existing Section 4 offence.
- Second, a pattern of behaviour creates "severe concern or distress" and significantly negatively impacts the victim's day-to-day activities. This aspect recognises the actual emotional and psychological suffering that stalking may inflict on victims, even if each incidence of stalker behaviour does not result in an express fear of violence.

Section 4A does not define the phrase "substantial adverse effect on, normal day-to-day activities", thus the courts will have to interpret it. The Home Office's Guidelines, however, suggest that evidence of a significant harmful effect might include the following:[23]

- the victim distorting their journey to work, shift patterns, or jobs;
- the victim organising for friends or relatives to pick up their children at school (to avoid contact with the stalker);
- the victim installing safeguards in their home;
- the victim shifting home;
- physical or mental ill-health;
- the victim's work performance degrading result of stress;
- the victim is ceasing or changing their social activities.

The critical distinction between Section 4 - Harassment and Section 4A - Stalking is that the latter adds a requirement, namely that the defendant's infringing behaviour causes the victim "severe anxiety or distress that has a major detrimental effect on their ordinary day-to-day activities". When there was insufficient evidence to show "fear of violence" in past occurrences and before the stalking statute, the only alternative was to file a summary charge. The added element under Section 4A, on the other hand, will allow prosecutors to consider an either-or offence. However, unlike the current Section 4 and the new Section 4A(1)(b)(i), the cumulative effect of the stalking is crucial, and no single incidence in the stalking needs to be particularly scary or dangerous. This is a crucial component of future offences. Prosecutors should evaluate the cumulative effect of stalking on the victim and the impact and type of individual events rather than focusing on particular instances.

4.2.1. Defence - Section 4A

In comparison to Section 2A, the Section 1(3) defences are expressly mentioned in Section 4A.

[23] 'Circular: Change to the Protection from Harassment Act 1997' (*Home Office*, 16 October 2012) 'http://www.homeoffice.gov.uk/about-us/corporate-publications-strategy/home-office-circulars/circulars-2012/018-2012/)

As set out in Section 4 A (3), there is a defence to stalking that includes fear of violence or severe amber alert or distress where it can be demonstrated that the course of conduct was:

- initiated for the intention of protecting or detecting crime,
- followed under any enactment or the rule of law; or,
- the striving of A's series of acts was reasonable for the safeguard of A or another or for protecting A's or someone else's property.

The perpetrator can face up to five years in prison for such conduct. The court can issue a prohibiting order according to Section 5 to prevent the perpetrator from contacting the victim again. Victims can also litigate in civil court to avoid future retaliation and recover damages. As a result of company molest of the Act, the Act has been attacked as a weapon for limiting free expression. The use of civil injunctions against peaceful demonstrators violates their right to free expression and protest.[24]

5. Judicial Interpretation

Prior to the 1997 law, there were a few notable UK court decisions in which stalking was brought under the umbrella of accusations such as "assault", "grievous physical injury", and "public annoyance". The offender was found guilty of inflicting grievous bodily harm on the victim through a campaign of silent phone calls by the Crown Court in *R* v. *Burston*[25]. The accused was blamed for the victim's depression. The ruling was affirmed by the Court of Appeals. The Court of Appeals in *R* v. *Ireland*[26] broadened the concept of assault by ruling that a sequence of calls followed by silence constituted assault. Assault is often characterized as when force is used immediately, nevertheless, the Irish Court has opened the possibility to attacks over a great distance. In *R* v. *Johnson*[27] The appellant Court affirmed an appellant's conviction of public annoyance for repeatedly making obscene phone calls during a five-and-a-half-year period. These unique rulings appear to be the result of the 1997 Act being motivated by the lack of a specific stalking provision.

In *Pratt* v. *DPP*[28], the Administrative Court ruled that two occurrences about three months apart were "close to the line", but nevertheless sufficient to demonstrate a course of conduct. However, courts have determined

[24] Liberty Central Law, 'Protection of Harassment Act, 1997' (*The Guardian*, 9 June 2009), <https://www.theguardian.com/commentisfree/libertycentral/2009/jun/01/liberty-central-protection-harassment> last accessed 11 November 2021
[25] *R v Burstow* (1996) Crim LR 331
[26] *R v Ireland* (1997) 1 All ER 112
[27] *R v Johnson* (1997) 1 WLR 367
[28] *Pratt v DPP* (2001) EWHC 483

that it is not merely the number of occurrences that constitute a course of behaviour, but whether those instances are sufficiently related to that and context to warrant the judgement that they constitute a course of conduct.[29]

6. Conclusion

Section 354D of the Indian Penal Code, which was amended in 2013, does not include all aspects of cyberstalking. The law makes no attempt to define "cyberstalking" or to clarify the meaning of "tracing the usage of any digital communication". The regulation commonly dealing the problem of invasion of privacy, it does now no longer covers different problems consisting of issuing threats or posting abusive remarks on digital media. It also dismisses the possibility of harassment by any third person as a result of the Stalker's actions. The Act's exclusions have yet to be confirmed as constitutional, and it will be intriguing to see how they are reconciled with Article 21's idea of a 'right to privacy'. Unlike United Kingdom law, Indian law does not provide for restraining orders, which would have provided the victim with additional protection.

In Conclusion, the 2013 amendment represents a step forward in the fight against cyberstalking, yet it is woefully inadequate. It places an unreasonable responsibility on the judiciary to interpret and reinterpret the legislative provisions to fit the facts of various case, and Section 354D independently will not provide the victim proper justice. It must be handled in combination with Section 69A of the Information Technology Act or any other applicable provisions of the Indian Penal Code, such as Section 499 and 503, to provide entire justice for the victim. As a result, the author believes India's cyberstalking laws has a numerous fault that must be solved before it can be deemed effective legislation.

[29] *Lau v DPP* [2000] Crim. L.R. 580; *See also*: *R v Patel* [2005] 1 Cr. App. 27