

**LEX SCRIPTA MAGAZINE OF LAW AND POLICY**  
**ISSN-**

**VOLUME-1 ISSUE-1**  
**YEAR: 2023**

**EDITED BY:**  
**LEX SCRIPTA MAGAZINE OF LAW AND**  
**POLICY**

All Copyrights are reserved with the Authors. But, however, the Authors have granted to the Journal (Lex Scripta Magazine of Law and Policy), an irrevocable, non-exclusive, royalty-free and transferable license to publish, reproduce, store, transmit, display and distribute it in the Journal or books or in any form and all other media, retrieval systems and other formats now or hereafter known.

No part of this publication may be reproduced, stored, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law.

The Editorial Team of Lex Scripta Magazine of Law and Policy Issues holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not necessarily reflect the views of the Editorial Team of Lex Scripta Magazine of Law and Policy.

[© Lex Scripta Magazine of Law and Policy. Any unauthorized use, circulation or reproduction shall attract suitable action under application law.]

**CRIMINAL LIABILITY FOR ONLINE HARASSMENT AND CYBERSTALKING**

**Author: Aditi Prasad, BBA.LLB(H) 2<sup>nd</sup> Year, Student of Amity University Ranchi,  
Jharkhand.**

**INTRODUCTION**

Recently, the rise of the internet has led to the upsurge in new forms of harassment and stalking, known as online harassment and cyberstalking. These forms of harassment can take many distinct forms, from sending threatening messages or spreading false rumours to tracking a victim's movements online or in real life. India has not only bagged one of the peak ranks for having the highest number of internet users, but we also ace the records of global sexual harassment. The harassment faced by women online reflects the image of harassment faced by them in real world. What is more striking is that instances of cyberstalking against men are on a surge. Experts have asserted that the ratio is 50:50 vis-à-vis the cases of cyberstalking faced by men and women. In response to the growing threat of cyber-crimes, governments around the world have enacted laws and regulations aimed at protecting individuals from online harassment and cyberstalking, and imposing criminal liability on perpetrators. This article explores the issue of criminal liability for online harassment and cyberstalking, examining the nature and prevalence of these crimes, the legal frameworks governing them, and the challenges of prosecuting and punishing offenders. Ultimately, it argues that a greater awareness of the harms of online harassment and cyberstalking, as well as stronger laws and enforcement mechanisms, are needed to protect individuals from these insidious forms of digital abuse.

**THE LEGAL DEFINITIONS OF ONLINE HARASSMENT AND CYBERSTALKING**

Internet harassment and cyberstalking are severe issues that have become more common as social media and digital communication have grown in popularity. While these acts can be extremely harmful to victims, the legal meaning of these offences varies depending on the country in which they occur.

To properly comprehend the nature of online harassment and cyberstalking, it is necessary to investigate the legal definitions of these offences. In general, online harassment is defined as a pattern of action that is meant to cause distress or harm to another person. Sending threatening or abusive messages, publishing sensitive or private information without authorisation, and creating phoney profiles or social media accounts to impersonate or harass someone are all examples of this.

Cyberstalking, on the other hand, is a more serious offence that involves persistent and intentional action that is intended to harass, intimidate, or threaten someone through the use of internet communication. This includes sending unwanted messages, following someone's online movements, and employing technology to stalk or watch someone in person. These offences' legal definitions might vary greatly depending on the jurisdiction in which they occur. These may be characterised as particular criminal acts in some circumstances, while others may come under broader categories such as harassment, stalking, or domestic abuse. Many jurisdictions have created legislation to handle online harassment and cyberstalking, recognising the unique nature of these crimes in the digital age. Prosecutors must generally prove that the perpetrator meant to cause injury or terror in the victim, that the victim had a reasonable fear of danger, and that the perpetrator's acts were the source of this fear in order to establish responsibility for online harassment and cyberstalking. They must also be able to identify the culprit, which might be difficult in circumstances where the attacker conceals their identity through anonymous accounts or other means. Ultimately, understanding the legal definitions of online harassment and cyberstalking is critical for properly dealing with these situations and holding perpetrators accountable. We may obtain a better grasp of the legal system in place to protect victims and prevent these behaviours from recurring in the future by reviewing the many definitions of these crimes and the legal requirements that must be met to establish responsibility. Online harassment and cyberstalking can both result in serious effects, such as emotional hardship, social isolation, and even physical damage. These acts are unlawful in many jurisdictions and can result in criminal prosecution or civil litigation. The definitions and penalties for online harassment and cyberstalking vary by country, but they often involve actions designed to cause harm or create a hostile environment for the victim.

### **TYPES OF ONLINE HARASSMENT AND CYBERSTALKING**

In the digital era, cyberstalking and online harassment are concerns that are growing more and more common. Numerous people report experiencing various types of online harassment, intimidation, and threats. To address the issue and hold offenders accountable, it is crucial to understand the many forms of online harassment and cyberstalking. Here are a few typical examples of cyberstalking and internet harassment:

- **Threats:** This form of internet harassment comprises making threats to damage a target person physically or psychologically. Threats can take many different forms, from overtly violent statements to subtle threats.

- **Doxxing**: It is the act of publishing or disseminating someone's personal information without that person's permission with the intention of hurting or embarrassing them. This may entail disclosing personal contact information, residential addresses, or even financial data.
- **Cyberbullying**: It is when someone intentionally and repeatedly bullies or harasses another person using electronic communication. This can involve saying offensive things, distributing false information, or posting embarrassing images or videos.
- **Revenge porn**: Revenge porn is the dissemination of pornographic material without the subject's permission. This can have detrimental psychological and emotional impacts can be done to shame, threaten, or embarrass the victim.
- **Stalking**: Whether done online or off, stalking entails persistent and unwelcome activity directed at a specific person. This can involve establishing unwelcome and persistent contact with the person or viewing, watching, or monitoring the person's actions.
- **Hate Speech**: The use of words or images with the intent to disparage, offend, or degrade is known as hate speech.

### **IMPACT OF ONLINE HARASSMENT AND CYBERSTALKING ON VICTIMS**

The victims of cyberstalking and online harassment are severely impacted. They may injure you physically, psychologically, and emotionally. Victims of abuse have occasionally even committed suicide as a result of the abuse they experienced. We will go into more detail about the effects of cyberstalking and online harassment on victims in this section.

- **Emotional discomfort**: Victims of cyberstalking and online harassment may experience severe emotional distress. They might experience anxiety, depression, and terror. As if they have no one to turn to for assistance, they could also feel hopeless and isolated. Relationships between victims and their friends and family may worsen as a result of the victim's isolation.
- **Psychological Trauma**: Online stalking and harassment victims may also experience psychological trauma. They may experience nightmares, flashbacks, and hyperarousal, which are all signs of post-traumatic stress disorder (PTSD). Moreover, they can have a hard time focusing, sleeping, and eating. Their general health and well-being may suffer as a result.
- **Physical Harm**: In some instances, cyberstalking and online abuse can cause victim's bodily pain. They may be the subject of physical attack, stalking, or threats of harm in person. Extreme circumstances could put sufferers in danger of death.

- Damage to Reputation: Cyberstalking and online abuse can seriously harm a victim's reputation. Online rumours or false charges can hurt a person's personal and professional relationships, possibly resulting in social exclusion, job loss, and relationship problems.
- Financial repercussions: Online stalking and harassment victims may potentially experience financial repercussions. To address the emotional and physical harm brought on by the abuse, they can be required to take time off work or shell out money for medical care. If they want to take the offender to court, they might also have to pay legal fees.
- Fear of Internet Activity: Those who have experienced cyberstalking or online harassment may develop a fear of using the internet or participating in social media. As a result, they might pass up crucial chances, such job interviews or social gatherings, further isolating them from society.
- Long-Term Effects: The effects of cyberstalking and online harassment can linger for a very long time. Years after the abuse has stopped, victims may continue to suffer from emotional pain, psychological trauma, and physical harm. They might also have trouble building relationships and trusting people, which would keep them socially isolated.

#### LEGAL JURISDICTIONS AND PUNISHMENTS:

Cyberstalking and online harassment are illegal in India and are subject to a number of statutes, including:

- Indian Penal Code (IPC) Section 354D<sup>1</sup> makes stalking, including online surveillance, a crime. If found guilty of cyberstalking, a person could face up to three years in jail and/or a fine.
- Information Technology Act, 2000:

This law includes provisions that make cyberstalking and online harassment illegal. Sending offensive messages via a communication device, including the internet, was illegal under Section 66A<sup>2</sup> of the Act, and offenders could face up to three years in jail and/or a fine. However, the Supreme Court of India invalidated this clause in 2015 because it was illegal.

- The 2013 Act for the Protection of Women from Sexual Harassment at Work:

---

<sup>1</sup> Indian Penal Code 1860

<sup>2</sup> Information Technology Act, 2000

This Act contains measures to safeguard women from workplace sexual harassment, including that which occurs online. Employers are required to set up an internal complaints committee to investigate and handle sexual harassment claims, including those made online.

- Juvenile Justice Act of 2015:

The Juvenile Justice Act of 2015 outlines provisions for the recovery of kids who have been harassed and stalked online. It also includes guidelines for dealing with those who harass and stalk minors online.

- The 2018 Criminal Law Amendment Act:

This Act modified the Indian Penal Code to establish penalties for those who harass and stalk women online. Three to five years in jail and/or a fine are possible penalties.

### **CRIMINAL LIABILITY FOR ONLINE HARASSMENT AND CYBERSTALKING**

Criminal liability for cyberstalking and online harassment refers to the possible penalties that the perpetrators of these crimes may experience. Online harassment is the act of intimidating, threatening, or harassing someone else through electronic communication. Cyberstalking is a term used to describe an ongoing pattern of online harassment that may also encompass offline stalker behaviour and involves threats or intimidation. Depending on the jurisdiction and the seriousness of the conduct, cyberstalking and online harassment are subject to varying degrees of criminal culpability. Online harassment may occasionally be charged as a misdemeanour, although more serious incidents may be charged as felonies. These crimes are punishable by fines, incarceration, and restraining orders. Identifying the appropriate jurisdiction to bring charges for cyberstalking and online harassment is one of the difficulties in doing so. It can be challenging to determine which law enforcement agency has jurisdiction to look into and punish certain offences because they can be committed across different jurisdictions. Also, it may be challenging to track down the offender of the crime due to the anonymity of online communication. The legal standard needed to establish these offences is another obstacle. Prosecutors must demonstrate that the behaviour was both undesired and caused the victim mental distress in order to show online harassment or cyberstalking. It may be challenging to establish this in court, especially if the offender asserts that their actions were intended as a joke or that they had no intention of causing harm. Notwithstanding these difficulties, there have been several examples of online harassment and cyberstalking that have been successfully prosecuted in recent years. For instance, in 2016 a guy was given a 14-year prison term for using several fictitious online identities to pursue and harass his ex-girlfriend. It is significant to highlight that cyberstalking and online harassment do not just apply to individuals.

Businesses that offer online communication platforms, including social networking websites, may also be held accountable if they do not take reasonable precautions to stop these crimes from happening on their platforms. These businesses could occasionally be obliged to assist law enforcement in locating those responsible for internet abuse and cyberstalking.

### **PREVENTION AND INTERVENTION STRATEGIES**

In order to address the issue of online harassment and cyberstalking, prevention and intervention techniques are essential. Criminal responsibility is a crucial tool for making offenders responsible for their acts, but preventative and intervention techniques can also help prevent these crimes from happening in the first place and offer support to victims. Education is a useful preventative tactic. Raising awareness of these problems and encouraging good online behaviour can be achieved by educating both kids and adults about the negative impacts of online harassment and cyberstalking. Children can be taught the value of digital citizenship and responsible behaviour online, and tools and assistance can be made available to those who have been the targets of online harassment and cyberstalking. The creation of policies and procedures for internet safety is another preventative measure. This may involve putting in place regulations outlawing cyberstalking and online harassment on social media sites and establishing precise procedures for reporting such violations. Also, social media corporations can create algorithms to find and delete content that is against their rules. In situations where cyberstalking and online harassment have already taken place, intervention measures can be especially crucial. The creation of victim support services is one efficient intervention technique. This can involve giving victims who want to file a lawsuit against their abuser's psychotherapy and therapy services as well as legal support. Using restraining orders is another intervention approach. A restraining order that forbids their attacker from contacting them either online or offline may be available in some circumstances for victims of cyberstalking and online harassment. This may be a powerful strategy for ending the harassment and giving the victim a sense of security. Finally, law enforcement organisations may be quite effective in stopping situations of online harassment and cyberstalking and stepping in to help. Investigating and pursuing perpetrators may be part of this, as well as offering victims assistance and resources. To identify and find the offenders, law enforcement organisations may cooperate with social media firms.

### **INTERNATIONAL PERSPECTIVES**

Cyberstalking and online harassment are global concerns that need to be addressed from a worldwide viewpoint. Because that the internet has no geographical boundaries, it is crucial to take a coordinated global strategy to solving these issues. We shall examine several

international viewpoints about criminal responsibility for online harassment and cyberstalking in this subtopic. The fact that cyberstalking and online harassment are frequently committed across national lines makes fighting these crimes difficult. It can be challenging to determine which jurisdiction should have control over a given matter because different nations have distinct laws and regulations. This can be particularly difficult when the victim and the attacker are from different nations. The United Nations and the Council of Europe are two international organisations that have taken steps to address the problem of online harassment and cyberstalking. In 2013, the UN issued a resolution stating that online abuse of women and girls violates those individuals' human rights. The member states were asked by this resolution to take action to stop and handle internet harassment and stalking.

Similar to this, the Council of Europe's Convention on Cybercrime provides a legal framework for dealing with cybercrime among its member countries, such as online harassment and cyberstalking. The Convention establishes safeguards for the rights of victims and calls on member states to work together to investigate and prosecute cybercrime. Many nations have created their own laws and regulations to deal with online harassment and cyberstalking in addition to international organisations. For example, in the United Kingdom, the Malicious Communications Act makes it a criminal violation to transmit a communication that is excessively offensive or threatening, with the goal to cause distress or worry to the recipient. In Canada, provisions for online harassment and cyberstalking were added to the Criminal Code in 2014. The modifications make it illegal to intimidate or harass someone online and allow for the issuance of peace bonds, which function similarly to restraining orders.

### **CONCLUSION**

In conclusion, cyberstalking and online harassment are severe offenses that can be extremely damaging to a person's mental and emotional health. Technology and social media platforms are being used more frequently, which has made it simpler for criminals to commit these offenses remotely and in secret. To hold these offenders responsible and give the victims justice, laws and regulations are in place in many countries around the globe. It's critical that people are informed of their legal options and how online harassment and cyberstalking are governed by local laws. As a community, we must work to establish a secure and welcoming space where people can access the internet without worrying about being harassed or stalked. We can prevent and fight online harassment and cyberstalking and ensure a safer and more equitable digital environment for everyone by educating ourselves on the legal repercussions of these crimes.