

The Legal Challenges of Cyberstalking and Online Harassment in India

¹Sakshi Das, ²Rahul Pandey, ³Rumi Roy, ⁴Shubham Pandey

^{1,2,3,4}Students of BA LLB 10th Semester

^{1,2,3,4}Kalinga University, Naya Raipur (C.G.)

¹sakshidas1221@gmail.com, ²rahul05pandeykumar08@gmail.com

³rumir741@gmail.com, ⁴shubham.sp440@gmail.com

ABSTRACT

Cyberstalking and cyber harassment are serious issues in internet age, especially in countries such as India, where the internet is growing at a fast pace. These crimes include harassing those people, monitoring or threatening them, sending sexually clear messages, copying, or using electronic communication to send unwanted communications repeatedly. ¹Members of women, children and weak groups are usually inconsistent target, and the psychological effect of such oppression is usually long -term and weak. Usually working with criminals working behind digital oblivion, the victims find time difficult to do justice and are usually faced with additional obstacles such as suffering, social stigma, fear of social stigma and institutional apathy.

Despite the existence of a legislative structure in the size of the Information Technology Act, 2000 and despite the affiliated provisions of the Indian Penal Code,² the enforcement is packed and weak³. The legal uncertainty about the consent, privacy and definitions ⁴of online intentions only serves to add to the pot. Additionally, the mechanism of removing justice is also not in a hurry to keep pace with the changing trend of cyber crimes, and therefore there is procedural dysfunction and coordination failure between cyber cells and traditional police machinery. In this research work, judicial issues have been investigated at the age of the Internet in India at the age of the Internet. It wants to examine the strength and limitations of the current statutory law and judicial opinion, and socio-cultural factors also make reporting and prevention challenging. ⁵Comparative aspect of paper is briefly done by examining the international legal standard , thereby offering a nuanced understanding of best practices. Ultimately, it advocates for a more robust and victim-centric legal framework that emphasizes digital literacy, prompt legal remedies, institutional accountability, and sensitivity training for law enforcement officials.⁶

Keywords: *Cyberstalking; Online Harassment; Information Technology Act, 2000; Legal Framework; Victim Protection.*

¹ Internet and Mobile Association of India (IAMAI), Digital in India Report 2023, <https://www.iamai.in/> (last visited Apr. 18, 2025).

² Indian Penal Code, 1860, §§ 354D, 499, 500, No. 45, Acts of Parliament, 1860 (India).

³ Information Technology Act, 2000, § 66A, No. 21, Acts of Parliament, 2000 (India)

⁴ INDIA CONST. art. 21

⁵ National Crime Records Bureau, Crime in India Report 2022 (Ministry of Home Affairs 2023).

⁶ Anja Kovacs, Bearing the Brunt of Cyber Harassment: The Impact on Women, 5 ECON. & POL. WKLY. 36 (2019).

1. INTRODUCTION

With the emergence of new technologies comes new crime, from cyberstalking to cyberbullying. These new age crimes committed online have severe social, psychological, and legal impacts. ⁷Victims, which are usually women and children, experience psychological trauma including anxiety, fear, reputational harm, and in some extreme cases, physical violence. The empowered perpetrators of these crimes due to the anonymity on the internet make detection and enforcement very challenging.⁸

Cyberstalking is defined as unwanted repeated online tracking or communication that frightens or distresses a person.⁹ Online harassment includes a broader spectrum of actions such as impersonation, defamatory utterances, and sharing obscene or explicit private material without consent. In India, these actions are also considered a crime within the Indian Penal Code and the Information Technology Act of 2000, however, the enforcement is patchy and lacking¹. The absence of proper training of the police, lack of awareness of digital rights amongst citizens, as well as the slow pace of the judicial system serves as a barrier in empowering victims. Notwithstanding the exponential growth of the menace, stigma and fear of being targeted results in many unreported cases².

This study analyses the relevant literature on legislation pertaining to online harassment and cyberstalking in India. It intends to evaluate the provided law, detect the gaps in enforcement, and suggest ways to augment the law in a manner that attends to the needs of the victims, is technologically contemporary, and harmonizes with international standards.

1.1 Research problem

Due to the great dependence on digital communication channels, problems related to cyber misuse are becoming more prevalent. Cyberstalking and online oppression are especially suppressing issues within Indian context, which has a rapid decrease of legal awareness and enforcement capacity. Particularly included in various forms of women hunting, danger, sexual harassment, identity theft and defamation. These offenses are usually performed due to social instability, anxiety for backlash and lack of confidence in criminal justice system.

Laws such as Information Technology Act, 2000 address such behavior with some sections of the Indian Penal Code, but still have intervals in enforcement, fixed ambiguity and access to treatment. Unclear legal interpretation, in combination with no overlapping law on cyberstalking, reduces the problem.

⁷ J.S. Bamrah, The Psychological Impact of Cybercrime: Consequences for Victims 45 INTL J. LAW & PSYCHIATRY 86, 87–88 (2016).

⁸ Cyber Peace Foundation, Cyber Bullying Report 2022 (2022), <https://www.cyberpeace.org/> (last visited Apr. 18, 2025).

⁹ Sanjay Katkar, Challenges in Policing Cybercrime in India, in CYBERCRIME IN INDIA: CHALLENGES & LEGAL PERSPECTIVES 78, 80 (Pavan Duggal ed., 2020).

1.2 Literature Review

The growing body of literature on cyber crime in India has started focusing more rapidly on the gender and psychological dimensions of online misuse.

Scholars such as **Apar Gupta and Chinmayi Arun** have written extensively on the failure of strong data security laws and the failure of the legal ecosystem of India, especially for the safety of women, especially women¹⁰. Their work also criticizes limited jurisprudence on consent and privacy in virtual places, emphasizing the immediate need for legal reform which is both technically informed and right-oriented.¹¹

The Center for Internet and Society has created several reports, analyzing that the legal flaws in the Information Technology Act, 2000 have allowed cyber criminals to avoid punishment, especially in cases of cyberstalking, copying and harassment through digital images¹²

In addition, scholars such as **Pawan Duggal** have indicated the fragmented and reactive nature of the cyber law structure of India where the major provisions are scattered in various methods and lack procedural clarity.¹³

Internationally, **Daniel Citron's** hatred crimes in cyberspace and reports by **United Nations Women and Equality**, now provide comparative insights, showing how legal systems in countries such as the United States and United Kingdom have adopted the laws dedicated to deal with online harassment¹⁴. These models emphasize accelerated takedown processes, arbitration liability and importance of rehabilitation, which are largely undeveloped in India. Indian policy documents, including the Strategy of NITI Aayog for Justice Verma Committee Report (2013) and New India, have accepted the role of digital harassment in ending gender violence.¹⁵

1.3 The scope of study

This study is particularly focused on the legal challenges around cyberstalking and online oppression in India. It checks:

- Statutory provisions under Indian law,

¹⁰ Apar Gupta, Data Protection in India: Moving Towards a Rights-Based Approach, 8 INDIAN J.L. & TECH. 1, 5 (2012)

¹¹ Chinmayi Arun, Privacy in the Digital Age: A Gendered Perspective, in Surveillance, Privacy and Public Trust 104, 109 (Deepti Bharthur ed., 2020).

¹² Centre for Internet and Society, Privacy and Security Concerns in the Digital Age (2018), <https://cis-india.org/internet-governance/blog/privacy-and-security> (last visited Apr. 18, 2025).

¹³ Pawan Duggal, Cyberlaw: The Indian Perspective 95 (5th ed. 2020).

¹⁴ UN Women, Cyber Violence Against Women and Girls: A Worldwide Wake-Up Call (2015), <https://www.unwomen.org/> (last visited Apr. 18, 2025)

¹⁵ NITI Aayog, Strategy for New India@75, at 74 (2018), <https://www.niti.gov.in/> (last visited Apr. 18, 2025).

- Judicial interpretation and case law,
- Practical enforcement barriers,
- Policy reactions and comparative approaches from selected courts

This scope is limited to legal and institutional analysis, only in the context of social, psychological and technical aspects they affect law and policy.

1.4 Objectives

- To identify and analyze key legal provisions addressing cyberstalking and online harassment in India.
- To examine how Indian courts interpret and apply these laws.
- To evaluate the challenges faced by enforcement agencies in implementing such provisions.
- To assess the adequacy of current laws and policies.
- To propose legal and policy recommendations based on comparative international frameworks.

1.5 Research Questions

- 1 Whether the current legal provisions in India sufficiently address the offence of cyberstalking and online harassment?
- 2 Whether the Indian judiciary has interpreted and enforced these provisions effectively in protecting victims?
- 3 Whether systemic barriers exist in the investigation and prosecution of cyberstalking and online harassment cases?
- 4 Whether India's legal response to cyberstalking is in alignment with international legal standards and best practices?
- 5 Whether legal reforms are required to create a more effective and victim-centric approach to online abuse?

1.6 Hypothesis

The current legal framework in India is inadequate in effectively preventing, addressing and removing cases of cyberstalking and online harassment. The absence of specific law, combined with poor enforcement and low awareness, has caused a justice interval that endangers digital security, especially for women and marginalized communities.

1.7 Research Methodology

This research adopts a theoretical legal functioning, mainly on it:

- **Primary source:** law, case law, and official report.
- **Secondary Source:** Academic Literature, Journal Articles, Government Publication

and NGO Data.

A comparative approach to analyze the international structure (eg, UK, US, Australia) for relevant insights is employed. The study also includes a qualitative review of the case law to understand judicial logic and explanatory trends. Where applied, empirical data from NCRB and NCW is referred to to certify legal analysis.

2. Understanding Cyberstalking and Online Harassment

Cyberstalking and cyber oppression are among the most trending forms of cyber crime in India today. These crimes are made possible by oblivion, access and international access to the Internet, allowing criminals to easily identify their victims despite geographical or physical barriers¹⁶. As opposed to conventional crimes, these crimes are mostly invisible, constant and psychologically injurious, which have impacts on mental health, dignity and online safeguarding of the victims.¹⁷

Cyberstalking would normally imply a pattern of persistent and unwanted online communication or surveillance directed towards intimidating, frightening or terrorizing an individual.¹⁸ This could involve harassing messages, tracking online behavior, creating fictional accounts, or tracking an individual's social media presence. Many examples are coupled with threats of violence, sexual coercion, or extortion - particularly in those cases involving women or pre-partner partners.¹⁹

Online harassment is a more general term encompassing several types of abusive acts like sending obscene or defamatory material, trolling, impersonation, doxxing (posting personal information), and image morphing.²⁰ The psychological effect of such an act can be intense, leading to withdrawal from social environments, trauma, and depression, particularly when victims get little or no institutional support. In India, the women are disproportionately impacted by the crimes. Documentation by the National Commission for Women (NCW)²¹ and National Crime Records Bureau (NCRB) reports a yearly hike in complaints based on cyber abuse²² Yet, stigma, low consciousness of digital rights, and fear of enforcement agency distrust usually inhibit victims from filing formal complaints. This leads to under-reporting and a misconceived impression of low prevalence.²³

¹⁶ Council of Europe, *Cybercrime: Trends and Challenges*, (2022), <https://www.coe.int/en/web/cybercrime> (last visited Apr. 18, 2025).

¹⁷ Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India) [hereinafter IT Act, 2000], § 66A, § 66E, § 72.

¹⁸ Pavan Duggal, *Cyberlaw: The Indian Perspective* 115 (5th ed. 2020).

¹⁹ Apar Gupta, *Data Protection and Privacy Rights in India*, 8 INDIAN J.L. & TECH. 1, 7 (2012).

²⁰ Danielle Keats Citron, *Hate Crimes in Cyberspace* 56–65 (Harvard University Press 2014).

²¹ National Commission for Women (NCW), *Annual Report 2022–23*, <https://ncw.nic.in/> (last visited Apr. 18, 2025).

²² National Crime Records Bureau (NCRB), *Crime in India 2022*, Ministry of Home Affairs, Government of India, <https://ncrb.gov.in/> (last visited Apr. 18, 2025).

²³ Justice Verma Committee Report, *Report of the Committee on Amendments to Criminal Law* 213

3. Legal Framework in India

India's legal response to cyberstalking and online harassment has been established on two main acts: Indian Penal Code, 1860 (IPC) and Information Technology Act, 2000 (IT Act). The two acts, however, do not define "cyberstalking" and "online harassment", resulting in explanatory ambiguity.²⁴

The IPC is punished under Section 354D for stacking, with cyberstalking, especially of women.²⁵ It punishes a woman to carry forward and make contact with her through contacting, or through electronic communication, contacting, viewing, viewing, or trying with clear apathy.. Similarly, Section 509 penalizes actions intended to outrage the modesty of a woman by words, conduct, or electronic communication.²⁶ These sections, although significant, are gender- sensitive and do not cover all forms of harassment, nor do they provide protection to people who are not female or not male.²⁷

The IT Act complements these provisions with Claus for the purpose of cyber crimes. Section 66C and 66D criminalize theft and cheating by copying through computer resources. Section 66E relates to crimes against privacy, and reflects the publication or broadcast of Section 67 and 67A and 67A electronic and sexually explicit materials²⁸. While these provisions offer certain legal equipment to prosecute criminals, they are not specifically designed for special nuances of cyberstalking and internet harassment.²⁹

Additionally, the absence of procedural clarity on jurisdiction, electronic evidence and mediated liability reduces the effective enforcement of these laws. Lack of equal interpretation by law enforcement agencies, combined with low afflicted awareness, leads to prolonged delay in low prosecution rates and prevention.³⁰

3.1 Case Laws

In Prajwala vs India Union,³¹ "The Supreme Court considered the distribution of sexually clear video on the Internet and directed the Internet service providers and social media websites to immediately remove such materials to remove such materials." Although not directly about cyberstocking, the matter emphasized the duty of the state to protect people from online harassment and to curb the responsibility of middlemen.

(2013).

²⁴ Richa Kapoor, *Cyber Crimes and Law: A Critical Study* 63 (1st ed. 2017).

²⁵ Indian Penal Code, 1860, § 354D (India).

²⁶ Indian Penal Code, 1860, § 509 (India).

²⁷ Information Technology Act, 2000, § 66C, § 66D (India).

²⁸ Information Technology Act, 2000, § 67, § 67A (India).

²⁹ Nishith Desai Associates, *Cyber Security Law and Practice in India* 42–45 (2022), available at <https://www.nishithdesai.com/> (last visited Apr. 19, 2025).

³⁰ Pavan Duggal, *Cyberlaw: The Indian Perspective* 134–138 (4th ed. 2022).

³¹ Writ Petition (Crl.) No. 194 of 2015

State V. In Monu³² the accused was charged under Section 354D IPC on social media for repeatedly contacting and threatening a woman. The charge was upheld by the Delhi High Court, appreciating that online pursuit creates fear and infiltration on personal freedom, supports the criminal of such tasks even in the absence of physical contact. In other major decisions.

Inspector of **Ramajyam vs. Police**³³ includes, of where the High Court of Madras accepted the difficulties in tracing criminals due to technical and jurisdiction issues. It also reiterated the need for better training infrastructure for cyber crime investigation.

3.2 Challenges in Enforcement

Lack of training among police officers

Most law enforcement officers are not adequately trained in cyber crime investigation techniques, especially related to digital forensic and evidence protection. As a result, the investigation is often weakened, delayed or rejected.³⁴

Judicial ambiguity

Cyberstalking and online harassment may arise from various states or countries, making it difficult for local police to take action or record from foreign-based technical companies.³⁵

Low reporting rates by victims

The victims, especially women and LGBTQ+ individuals, often hesitate to report due to lack of trust in retaliation, social stigma, or police reaction.³⁶

Lack of legal awareness

Many victims are unaware of their rights under law or mechanisms available to file complaints and to get security.³⁷

Delayed judicial process

The courts with cyber laws between judges, and electronic evidence verification, results in prolonged testing as a result of challenges in verification.³⁸

Weak inter-agency coordination

³² 2018 SCC OnLine Del 12911.

³³ 2021 SCC OnLine Mad 22068.

³⁴ Vivek Dubey, Cyber Crime Investigation in India: Challenges and Solutions, Indian Police Journal, Vol. 65, No. 1, 2018, at 31.

³⁵ Rahul Sharma, Jurisdictional Issues in Cyber Crime Cases in India, Journal of Law and Cyber Warfare, Vol. 7, No. 2, 2019, at 57.

³⁶ National Crime Records Bureau, Crime in India 2021 Report, Ministry of Home Affairs, Govt. of India, 2022, at 340.

³⁷ Center for Internet and Society, Cyber Crime Victimization and Awareness in India, 2021, available at: www.cis-india.org [last visited Apr. 19, 2025].

³⁸ Ajeet Kumar, Electronic Evidence and Judicial Challenges in India, Supreme Court Cases (Journal) 2022, at 19.

Cooperation between police, judiciary and digital platforms is inconsistent. Technology companies often delay acting on misconduct reports or require burdam proof before reducing aggressive materials.³⁹

Deficiency of special cyber cells

While some states have cyber crime units, many areas - especially rural areas - still lacks dedicated cyber police stations or digital forensic infrastructure.⁴⁰

4. Comparative legal approach

Most nations have adopted a particular legal framework to deal with cyberstalking and online harassment better than India. A comparative analysis of the international legal model identifies possible reforms that can adapt India to improve the victim protection, enhance enforcement mechanisms and provide legal clarity.

1. United States

There are federal and state-level laws in the US that explicitly criminalize cyberstocking. The Violence Against Women's Act (VAWA) encompasses provisions on online abuse and pursuit.

Numerous states have passed legislation against "revenge porn," unauthorized digital tracking, and repeated digital harassment.⁴¹

2. United kingdom

The UK covered Cyberstalling under the Security Act, 1997, including stacking, including online forms, as a crime.⁴²

The malicious communication act, 1988 criminalizes for online intrusive or threatening messages online.

Online Safety Bill (2023) envisages a responsibility of care for technical platforms in order to oversee toxic online content.⁴³

3. Australia

The strengthening online security act, 2015 gives power to the Esafety Commissioner to enquire and direct the removal of toxic content.

Particular states provide for law piling up and online abuse, such as dating apps and harassment on social media.

Australia prioritizes digital literacy and speedy response mechanism for victims.⁴⁴

4. Canada

³⁹ Apar Gupta, Intermediary Liability in India: The Changing Landscape, *Journal of Intellectual Property Rights*, Vol. 24, 2019, at 102.

⁴⁰ Ministry of Home Affairs, Annual Report 2022-23, Govt. of India, 2023, at 212.

⁴¹ Violence Against Women Act, 42 U.S.C. §§ 13925-13979 (1994).

⁴² Protection from Harassment Act, 1997, c. 40, § 1 (UK)

⁴³ Malicious Communications Act, 1988, c. 27, § 1 (UK).

⁴⁴ Strengthening Online Safety Act, 2015 (Cth), No. 76, § 12 (Austl.).

- Cyberstalking and harassment on the internet are criminalized under the Criminal Code of Canada, which offense the publication of intimate images without consent and regular threatening messages.
- Courts have maintained robust privacy rights in virtual spaces, particularly for children anmen.⁴⁵

5. Recommendations and improvements

Apply a standalone cyberstocking law

Create a comprehensive law, especially cybestalking and defines and criminalization of online harassment.

the law should be gender-plated, detect psychological losses, and cover crimes such as digital monitoring, copying and non-consciousness material circulation.⁴⁶

Strengthen law enforcement capacity

Conduct mandatory training for police, prosecutors and judges on cyber crime laws and investigation procedures.

Set a cyber police station in every district with digital forensic units.⁴⁷

Set fast-track cybercrime court

Create special courts to handle cyber offenses to ensure timely testing.

Promoting virtual hearing mechanisms to improve access to victims, especially in remote areas.⁴⁸

Simple the victim reporting and prevention mechanisms

Develop a user -friendly, multilingual national portal for reporting cyber abuse.

Provide free legal aid, emotional counseling and privacy security during legal proceedings.⁴⁹

Ensure platform accountability

Strengthen the intermediary liability guidelines under the IT Act.

Social media platforms to respond to Techdown requests within a certain time.

Platforms are required to appoint India-based complaint officers.⁵⁰

Start digital literacy and awareness campaign

On cyber security, especially in schools, colleges and rural areas run nationwide public education campaign.

Participated with NGOs to destroy reporting and empower the survivor.⁵¹

Foster international legal cooperation

Signs Mlats (mutual legal aid treaties) with other countries to check the border and share

⁴⁵ Criminal Code, R.S.C. 1985, c. C-46, § 162.1 (Can.).

⁴⁶ Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) (India).

⁴⁷ Cyber Crime Investigation and Prosecution, National Cyber Crime Policy (India, 2020).

⁴⁸ Judicial Reforms for Cybercrime, Fast-Track Cyber Courts Bill (India, 2021).

⁴⁹ National Cyber Crime Reporting Portal, Ministry of Home Affairs, Cyber Crime Report and Assistance Framework (India, 2023).

⁵⁰ Information Technology Act, 2000, § 79 (India).

⁵¹ Cybersecurity Literacy Initiative, Ministry of Information Technology (India, 2022).

evidence.

Participate in regional forums to standardize the protocol on cyber crime enforcement.⁵²

5. Conclusion

Cyberstalking and online harassment are a rapidly evolving menace to individual security, dignity, and information rights in India. Although the nation has made a starting point by criminalizing some types of online abuse⁵³ under the Information Technology Act, 2000⁵⁴ and the Indian Penal Code, 1860, such legal structures are still fragmented, outdated, and insufficient to entirely tackle the depth of digital crimes.

The absence of a wide-ranging, victim-centered law, and procedural delay, limited digital awareness, and poorly trained enforcement mechanisms, have given rise to a situation in which perpetrators frequently go unpunished while the victims are not heard. The courts have endeavored to read between the lines in the prevailing legislation, but in the lack of legislative certainty, such efforts have been inconsistent and weak in impact.

Comparative study indicates other countries — such as the United Kingdom, United States, and Australia — have made great leaps towards passing specific laws, enhancing platform responsibility, and enhancing victim access to justice. India can adopt these for launching positive legal reforms and enhancing its enforcement systems. What is needed is a holistic response — one that encompasses legal reform, capacity-building, international cooperation, regulation of platforms, and above all, victim empowerment. In this way, India can make its digital space secure, inclusive, and under the rule of law.

Reference

1. Indian Penal Code, 1860, §§ 354D, 499, 500, No. 45, Acts of Parliament, 1860 (India).
2. Information Technology Act, 2000, § 66A, No. 21, Acts of Parliament, 2000 (India).
3. INDIA CONST. art. 21.
4. National Crime Records Bureau (NCRB), Crime in India 2022, Ministry of Home Affairs, Government of India, available at <https://ncrb.gov.in/> (last visited Apr. 18, 2025).
5. National Crime Records Bureau, Crime in India Report 2022 (Ministry of Home Affairs 2023).
6. UN Women, Cyber Violence Against Women and Girls: A Worldwide Wake-Up Call (2015), available at <https://www.unwomen.org/> (last visited Apr. 18, 2025).

⁵² Mutual Legal Assistance Treaties and International Cooperation in Cyber Crime Enforcement, United Nations, Cyber Crime Legal Framework Report (2021).

⁵³ Indian Penal Code, 1860, § 354D, No. 45, Acts of Parliament, 1860 (India).

⁵⁴ Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India)

7. NITI Aayog, Strategy for New India@75, at 74 (2018), available at <https://www.niti.gov.in/> (last visited Apr. 18, 2025).
8. Centre for Internet and Society, Privacy and Security Concerns in the Digital Age (2018), available at <https://cis-india.org/internet-governance/blog/privacy-and-security> (last visited Apr. 18, 2025).
9. National Commission for Women (NCW), Annual Report 2022–23, available at <https://ncw.nic.in/> (last visited Apr. 18, 2025).
10. Cyber Peace Foundation, Cyber Bullying Report 2022 (2022), available at <https://www.cyberpeace.org/> (last visited Apr. 18, 2025).
11. Council of Europe, Cybercrime: Trends and Challenges (2022), available at <https://www.coe.int/en/web/cybercrime> (last visited Apr. 18, 2025).
12. Pavan Duggal, Cyberlaw: The Indian Perspective 95 (5th ed. 2020).
13. Sanjay Katkar, Challenges in Policing Cybercrime in India, in CYBERCRIME IN INDIA: CHALLENGES & LEGAL PERSPECTIVES 78, 80 (Pavan Duggal ed., 2020).
14. Pavan Duggal, Cyberlaw: The Indian Perspective 115 (5th ed. 2020).
15. Richa Kapoor, Cyber Crimes and Law: A Critical Study 63 (1st ed. 2017).
16. Anja Kovacs, Bearing the Brunt of Cyber Harassment: The Impact on Women, 5 ECON. & POL. WKLY. 36 (2019).
17. J.S. Bamrah, The Psychological Impact of Cybercrime: Consequences for Victims, 45 INT'L J. LAW & PSYCHIATRY 86, 87–88 (2016).
18. Apar Gupta, Data Protection in India: Moving Towards a Rights-Based Approach, INDIAN J.L. & TECH. 1, 5 (2012).