



CYBERCRIME AGAINST WOMEN: Legal Frameworks, Emerging Challenges, and Policy Responses

Gunjan Basrani¹ | Ms. Alpika Shrivastava²

¹ LL.M, 2nd Semester, Student at Jagannath University, Jaipur, Rajasthan (India).

¹ Assistant Professor of Law, Jagannath University, Jaipur, Rajasthan(India).

I. ABSTRACT

The advent of digital technologies continually transforms the methods through which abuse takes place, predominantly targeting women. Cyberbullying, comprising the delivery of threatening messages using messaging platforms, spying without consent, uploading pictures without permission, identity fraud, extortion of explicit photos/videos, and disseminating private data among others aims at undermining the most fundamental human rights of dignity, freedom, and expression. Through an evaluation of the type, extent, and gendered character of these violations, it becomes evident that the legal measures established in order to secure individuals from any form of harm fall short of their mark. International law, as assessed, suffers from a number of shortcomings, including weaknesses in enforcement and inconsistency. Data and judicial rulings have revealed problems within the framework of law itself rather than its effectiveness in curbing cyberbullying. Victims often have a hard time accessing resources for help not due to their own fault, but by the way these systems themselves are constructed.

II. KEYWORDS

cybercrime, gender-based violence, online harassment, cyberstalking, non-consensual pornography, digital rights, information technology law.

III. INTRODUCTION

The internet, which was once seen as an avenue of equality through digital means, has ended up becoming yet another avenue of reinforcing social inequalities. Women and young girls who have long been oppressed socially now find themselves facing another form of oppression, cyber violence against them.³ Online gender-based harassment, according to the World Economic Forum, is responsible for the digital gender gap that limits the participation of women in political and economic areas.⁴

¹ LL.M, 2nd Semester, Student at Jagannath University, Jaipur, Rajasthan (India).

² Assistant Professor of Law, Jagannath University, Jaipur, Rajasthan(India).

³ United Nations Office on Drugs and Crime (UNODC), "Cybercrime and Gender-Based Violence" (2021), available at <https://www.unodc.org/unodc/en/cybercrime/index.html>.

⁴ World Economic Forum, Global Gender Gap Report 2022 (Geneva: WEF, 2022), p. 7.

A multitude of cybercrimes targeting women exists in many ways, including harassment through the internet as well as violence within homes with the involvement of modern technologies. For instance, in the 2020-2022 period in India, according to NCRB data, there is an increase in cybercrimes by 24.4 percent. Women have been the victims in crimes relating to obscene content and stalking on the Internet.⁵ While the issue of cyber-crime against women is understood well at present, legislative approaches to the problem remain insufficient and fail to take into consideration victims' concerns and experiences. In order to address the issue, Danielle Citron argues that cyber abuse should be viewed from the perspective of civil rights violations rather than simply bad manners. This study is aimed at the examination of cybercrime against women and its aspects.

A. RESEARCH OBJECTIVE

- To understand the kind of crimes that are being committed against women online along with their dynamics.
- To discuss briefly about the legislations that have been enacted in India to combat the problem of cybercrimes against women.
- To discuss the effectiveness of cybercrime laws both internationally and at home.
- To analyze the problems faced by female victims when reporting cybercrimes.
- To examine the consequences of cybercrimes on the privacy, self-respect, mentality, and participation of the women victim in society.
- To discuss what has been done by internet forums, police stations, governments, and many other organizations to solve the issue of cybercrimes against women.
- To conduct a comparative analysis of the policies related to cybercrimes against women around the globe.
- To identify some of the measures which could be taken in order to improve the existing scenario.

B. RESEARCH QUESTIONS

- Are there enough legal provisions in India for tackling cybercrime against women and providing protection to the victims?
- How many different types and dimensions of cybercrime can target women in the cyberspace?
- How can Indian legal provisions related to cyber laws aid in tackling the problem of cybercrime against women?
- What are some of the impediments that prevent the victims from filing cases against the offenders?
- What effects can cybercrime have on women victims' privacy, dignity, mental well-being, and right to use the internet?
- How can digital intermediaries contribute to the prevention of cybercrime against women?
- How can we benefit from international laws related to cybercrime and apply it to Indian context?
- What are some possible recommendations for dealing with cybercrime against women from a legal and policy perspective?

C. HYPOTHESIS:

The existing legal framework and policy mechanisms in India are not sufficient enough to effectively address cybercrime against women because of certain legal and technical difficulties.

⁵ National Crime Records Bureau (NCRB), Crime in India 2022 (New Delhi: Ministry of Home Affairs, 2023), Chapter 5A.

D. RESEARCH METHODOLOGY

This study will adopt doctrinal research methodology to discuss the problem of cybercrime against women in India, paying special attention to legal aspects and emerging challenges, as well as to policy mechanisms. This paper will be mainly based on the use of secondary data sources, which include statutory laws, judicial precedents, books, journal articles, research papers, government reports, committee reports, and international conventions dealing with issues of cyber law and women's rights.

E. LITERATURE REVIEW

The recent literature on cybercrime against women underlines that digital technologies have converted traditional forms of violence into modern online dangers that excessively affect women. The primary focus of early study on cybercrime was pertaining to technical and regulatory aspect; nonetheless, there is soaring recognition in recent times of cybercrime against women as a gendered issue involving harassment, cyberstalking, online abuse, identity theft, sextortion, and non-consensual sharing of intimate images. Researchers have contended that digital realm often creates social inequalities which makes women prone to online abuse and violence.

A number of studies on cyber stalking and cybercrime against women from feminist and criminology perspectives have been carried out. The main thing is that cyber abuse should be perceived as a grave violation of a person's private life and his/her dignity. As studies state, the representatives of women who perform important roles within society such as journalists, activists, and professionals are usually exposed to online attacks intended to silence them on the Internet. Moreover, literature demonstrates that gender relations and structures of society have a great impact on cybercrime rates.

This research theme about image-based sexual abuse and non-consensual dissemination of intimate images has received much attention in academia. Authors argue against phrases such as "revenge pornography" because they are too restrictive and victim blaming; they propose alternative frameworks to recognize different instances of image-based sexual abuse. Research suggests that victims endure numerous psychological, emotional, and social consequences, including fear, depression, damage to reputation, and isolation from digital interactions. The use of emerging technologies, such as deepfakes and artificial intelligence, poses additional challenges for regulations.⁶

Many researchers have examined the legal aspects related to cybercrime against women. It is seen by researchers that although the laws such as the Information Technology Act and certain criminal laws are relevant to certain offenses, they fall short when dealing with new forms of offenses in the digital world. Comparisons indicate that nations that have enacted laws specifically related to cyber harassment, cyberstalking, and cyber image offenses handle matters better than nations that only apply criminal laws to their cases.

Moreover, the literature on platform governance and institutional reactions suggests that social media corporations and other forms of digital intermediaries have a significant part to play in facilitating or inhibiting cyber abuse. According to scholars, ineffective content moderation, late reaction to complaints, and inadequate accountability contribute to the occurrence of abuse. Research literature also reveals that

⁶ Dragiewicz, Molly, et al. 'Technology Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms.' *Feminist Media Studies* 18(4) (2018): 609–625.

victims encounter obstacles in the form of victim-blaming attitudes, lack of digital skills, and insensitivity within institutions, which makes them reluctant to report and get help.

However, there are certain lacunae in the literature despite its increased presence. The first problem concerns the fact that much of the research conducted focuses on Western areas with minimal attention paid to developing nations. The other problem is that there has been no intersectional approach taken in understanding the effects of different aspects such as socio-economic standing, caste, geography, and educational background in influencing cybercrime vulnerability.

IV. TYPOLOGY OF CYBERCRIME AGAINST WOMEN

4.1 Online Harassment and Trolling

The online harassment is an activity that repeats itself and happens without consent on the part of the individual, with the aim of harassing, intimidating, or making the life of the other person unbearable by damaging his/her reputation or otherwise. Trolling is a form of online harassment where messages sent with the purpose of offending, threatening, or abusing the other are included.

4.2 Cyberstalking and Doxing

Cyberstalking is the use of any form of electronic communication to stalk, monitor, or threaten an individual to the point where the victim fears for his/her safety. Cyberstalking is a stand-alone phenomenon, but it can be committed together with the broader intimate partner violence against the individual.⁷ Doxing is the exposure of personal data about the victim, such as her/his address or number.

4.3 Non-Consensual Intimate Image Sharing (NCII)

The distribution of intimate images of any person without the person's consent constitutes non-consensual intimate image sharing, better known as "revenge porn." The Cyber Civil Rights Initiative reports that 90 percent of non-consensual intimate image sharing victims are females. Most of them are exposed to mental distress that can manifest itself in the form of anxiety, depression, and post-traumatic stress disorder.⁸

4.4 Sextortion

Intimate images or threats to distribute them are used to exploit people financially, sexually, or relationally in sextortion. This offense involves deception in acquiring images and causes mental distress in its victims.

4.5 Cyberbullying

Cyberbullying is a problem that concerns individuals of both sexes, although studies show that it has different effects depending on the gender of victims. It was discovered that girls are victims of relational, sexual, and identity-oriented forms of bullying more frequently than boys. Cases of severe cyberbullying have been shown to result in self-injury and suicidal ideation in girls.⁹

4.6 Technology-Facilitated Intimate Partner Violence

New forms of abuse are being used by abusers against their partners with the help of digital technology. Technology-enabled intimate partner violence is the use of technology to monitor or control the partner with the addition of any form of physical abuse.

⁷ Lenhart, Amanda et al., "Online Harassment, Digital Abuse, and Cyberstalking in America," Data and Society Research Institute (2016), p. 14.

⁸ Cyber Civil Rights Initiative, "2019 CCRI Survey Results," available at <https://cybercivilrights.org/ccri-2019-survey/> (accessed May 2025).

⁹ Hinduja, Sameer and Justin W. Patchin, "Bullying, Cyberbullying, and Suicide," *Archives of Suicide Research* 14(3) (2010): 206–221.

V. SCALE AND EMPIRICAL DATA

The problem of cybercrime against women is hard to measure due to under-reporting issues, lack of standard definition, and absence of gender-specific statistics. Despite these factors, there is enough information to conclude that the problem is rather serious. According to a 2016 survey conducted by the Data and Society Research Institute, 47 percent of women aged 18-29 have been victims of cyber-harassment in the United States.

A global 2020 survey performed by Plan International on 22 countries revealed that one in five girls have decided to stop or limit their social media use due to online harassment. Moreover, according to EIGE estimates, cyber violence affects 4-7 percent of women per year in the EU, the largest group of which are young females.¹⁰

According to the 2022 data provided by the National Crime Records Bureau of India, numerous cases of cyber-related crimes committed against females have occurred, including online harassment, obscene communication, and violation of privacy, among others. Nevertheless, experts believe that the reality is even worse.

The worrying aspect from various studies conducted has been what is termed as the chilling effect of cyber abuse. Those women who experience online abuse tend to hold back on how much they express themselves through cyberspace, thus withdrawing from various online platforms.¹¹

VI. LEGAL FRAMEWORK

6.1 The Indian Legal Framework

The major act relating to cybercrime is the Information Technology Act, 2000 (IT Act) that was further updated in 2008. Some of its major sections are Section 66 (violation of privacy), Section 66C (identity theft), Section 67 (obscene content), Section 67A (sexual content) and Section 67B (child pornography).¹²

Another important amendment in Indian law relating to cyber-crimes is the Criminal Law (Amendment) Act, 2013, where the Indian Penal Code, 1860 was amended to add gender-oriented laws. These included Section 354A (sexual harassment), Section 354C (voyeurism) and Section 354D (stalking, including cyberstalking).¹³

There has been no provision in Indian law prohibiting NCII till date, which makes it an area of concern. One important case relating to the Information Technology Act was that of Shreya Singhal v. Union of India, which reduced the applicability of Section 66A.¹⁴

6.2 International Legal Instruments

On an international scale, the Budapest Convention on Cybercrime (2001) is one of the most complete agreements for cooperation regarding cybercrimes. It does not, however, deal with gender-based cyber-violence.¹⁵

¹⁰ European Institute for Gender Equality (EIGE), "Gender-Based Cyberviolence: A New Challenge for the EU" (2017), p. 21.

¹¹ *ibid*

¹² Information Technology Act, 2000 (India), as amended by the Information Technology (Amendment) Act, 2008.

¹³ Indian Penal Code, 1860, §§ 354A, 354C, 354D, 499, 500 (as amended by the Criminal Law (Amendment) Act, 2013).

¹⁴ Shreya Singhal v. Union of India, (2015) 5 SCC 1 (Supreme Court of India).

¹⁵ Budapest Convention on Cybercrime (Council of Europe Treaty Series No. 185), opened for signature 23 November 2001, entered into force 1 July 2004.

The UN Special Rapporteur on violence against women has requested that States put into place detailed legislation dealing with technology-based gender-based violence.¹⁶ There are some countries that have shown the lead by legislating specifically regarding gender-based cyber violence. The UK implemented the law regarding revenge pornography under the Criminal Justice and Courts Act 2015, while recently introducing the Online Safety Act 2023. Australia's eSafety Commissioner deals with NCII complaints, and Scotland has implemented legislation for sharing images without consent under the Abusive Behaviour and Sexual Harm (Scotland) Act 2016.¹⁷

6.3 Platform Liability and Self-Regulation

Role of social media and communication platforms in both facilitating and preventing crimes against women through the cyberspace is critical. The safe harbor principle as provided under Section 230 of Communications Decency Act of US and Section 79 of IT Act of India has always been a shield to such platforms.

VII. JUDICIAL APPROACH TOWARDS CYBERCRIME AGAINST WOMEN

Indian courts have contributed immensely towards protecting women from cybercrimes through their interpretation of constitutional rights and their efforts towards providing privacy to individuals. The use of technology can lead to violation of the dignity and privacy of women; hence, it becomes the responsibility of the courts to provide adequate solutions. Offences committed through cyber space may have serious effects on the life of the victim.

7.1 Recognition of Privacy and Dignity as Fundamental Rights

The most important judicial development in this context is the acknowledgment of the right to privacy as a fundamental right. According to the case of Justice K.S. Puttaswamy v. Union of India¹⁸, the Supreme Court ruled that privacy is an inherent aspect of the right to life and personal liberty guaranteed under Article 21 of the Constitution. It was established in this landmark judgment that informational privacy and data protection have become indispensable needs of the modern digital era.

Such a judgment has great significance for cybercrimes committed against women, including but not limited to revenge pornography, the circulation of nude images without permission, stalking, and identity fraud.

7.2 Balancing Freedom of Speech and Online Safety

Shreya Singhal vs Union of India¹⁹ is an instance wherein Section 66A of the Information Technology Act, 2000 was declared unconstitutional by the Supreme Court of India for placing arbitrary restrictions on freedom of speech and expression.

In its judgment, while protecting the right to freedom of speech and expression, the court made it clear that any threat, obscenity, harassment, defamation, or incitement carried out through online activities would be punishable as per other legal provisions.

7.3 Early Convictions in Cybercrime Cases

The most important case in the context of cyber laws in India is the State of Tamil Nadu v. Suhas Katti²⁰. Here, the accused had fabricated some statements against the woman online. He did this by creating some

¹⁶ UN General Assembly, Report of the Special Rapporteur on violence against women, its causes and consequences, UN Doc. A/HRC/38/47 (2018).

¹⁷ Slane, Andrea, "Sexting and the Law in Canada," Canadian Journal of Human Sexuality 22(3) (2013): 117–122.

¹⁸ Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors. (2017) 10 SCC 1

¹⁹ Shreya Singhal vs Union of India (2015) 5 SCC 1

²⁰ State of Tamil Nadu v. Suhas Katti CC No. 4680 of 2004

derogatory and defamatory posts about the woman in question on internet discussion forums. The accused was found guilty under the IT Act.

This case is also considered among the first few cases where an individual in India could be charged for committing cybercrimes.

7.4 Protection Against Obscene and Non-Consensual Content

Indian courts have time and again disapproved of the use of and distribution of obscenity in regard to women. Judicial pronouncements have stated that the use of intimate photos and videos by individuals without their consent is a breach of one's dignity and privacy rights.

In some cases of the abuse of social networking sites, the courts have taken into account the serious mental and social harm caused by the use of such pictures and videos on individuals without their consent.

Courts have also advocated the use of Section 67 and 67A of the Information Technology Act when sexually explicit materials are involved.

7.5 Judicial Recognition of Cyberstalking

The offense of stalking, both traditional and electronic or cyber-stalking, has been the subject of much judicial consideration. The courts have realized that continuous electronic surveillance, threats, persistent unwanted contact, and harassment can cause fear and anxiety to a woman.

Cyber-stalking has been regarded as an offense that threatens the security and liberty of a woman. Technology should not be made an instrument of fear and harassment.

7.6 Protection of Women's Dignity in the Digital Sphere

It has been emphasized in Indian courts that the dignity of women needs to be respected regardless of the space where the crime is committed, be it virtual or physical. The courts have interpreted the right under Article 21 to include the right to lead a dignified life with honor and reputation.

In matters relating to the creation of false profiles, image morphing, online defamation, and cyber fraud, courts have observed that such activities may affect the woman's dignity in her professional and private life. Accordingly, the courts have recommended that cases of this nature be investigated and prosecuted promptly.

7.7 Judicial Response to Advancing Technology

The rise of artificial intelligence and deepfakes poses new challenges for courts to deal with instances of cyberbullying. Though specific laws related to deepfakes do not exist yet, judicial pronouncements clearly point out that there is an increased recognition of the threats from AI technologies.

It has been stressed that there should be effective regulations to curb the creation of fabricated sexually explicit content of women through advances in AI technologies.

VIII. STRUCTURAL BARRIERS TO JUSTICE

8.1 Under-Reporting and Victim-Blaming

Cybercrime against women is also frequently under-reported due to social stigma, mistrust in the police, fear of retribution by the offenders, and fear of victim-blaming.²¹

8.2 Evidentiary Problems

Obtaining and keeping electronic evidence is technologically difficult, requiring specialist knowledge not found among many police forces. International Mutual Legal Assistance Treaty processes for obtaining evidence from another state take too long to make them viable options in an emergency situation.

8.3 Lack of Consistent Definitions and Jurisdictional Fragmentation

The lack of a global standard for defining cybercrime against women results in inconsistencies in the way that such crimes are categorized, prosecuted, and punished across geographical areas. Such problems are compounded when the offender is located in one state while the victim resides in another.

8.4 Digital Divide and Economic Disadvantage

Victims who belong to marginalized groups often have additional obstacles in getting justice in cases of cyber-crime. Limited digital literacy makes it difficult for victims to collect evidence, file complaints, or obtain legal counsel. Several forms of discrimination increase the vulnerability of such victims.²²

IX. RECOMMENDATIONS FOR REFORM

9.1 Legislative Reform

Specific legislation is needed to make the crimes of NCII and sextortion criminal. It would be helpful for India to have a general law such as the Cyber Safety and Digital Rights Act, which includes specific provisions, specifies victim-specific offences, and creates a special court for cyber-related offences.

9.2 Police Response Capacity

The police must undertake mandatory training in how to investigate cybercrimes, taking into account gender sensitivity when interviewing victims and collecting digital evidence. Each district must have a special unit within the police force responsible for investigating gender-based crime.

9.3 Internet Service Provider Accountability

It will be necessary for governments to review the safe harbors provided by the laws, allowing conditional immunities where providers do not qualify unless they are able to detect and remove illegal gendered content from their sites.

9.4 International Cooperation

States should ratify and put in place the Budapest Convention and work towards adopting an extra protocol aimed at tackling cyber abuse based on gender. MLAT procedures must be expedited using electronic means.

9.5 Support for Victims and Civil Society

²¹ Jane, Emma Alice, *Misogyny Online: A Short (and Brutish) History* (London: SAGE Publications, 2017), p. 44.

²² Vera-Gray, Fiona, "Men's Stranger Intrusions: Rethinking Street Harassment," *Women's Studies International Forum* 65 (2017): 9–17.

Legal and psychological assistance aimed at victims of cyber abuse must be funded. Organisations involved in civil society in this field must continue receiving government funding as well. Education programmes need to incorporate digital literacy and consent education from an early age.²³

X. CONCLUSION

Cybercrime against women is one of the most important human rights issues in the modern digital era. Such crimes prevent women from exercising their personal freedoms, silence their voices, and perpetuate existing forms of social inequality. The presented analysis demonstrates that even though legislative initiatives have been implemented and strengthened since 2013 in India and on an international level, there are considerable weaknesses in current policies in the area.

Based on the stated research objective and questions formulated at the beginning of this paper, the hypothesis is confirmed. Specifically, legislative efforts in the discussed area are currently insufficient as they have been developed without taking into account gendered dynamics in cybercrime. In addition, the presented evidence fully supports the subsidiary hypotheses formulated previously.

Efforts required for addressing the identified problem should be comprehensive in nature and include effective legislation and law enforcement, platforms' responsibilities, international cooperation, and provision of education to female users as well as victims of online violence. In essence, changes required include a shift in mentality regarding cybercrimes against women as genuine cases of abuse.

XI. REFERENCES

1. Amnesty International. 'Toxic Twitter: A Toxic Place for Women.' 2018. Available at: <https://www.amnesty.org/en/research/2018/03/online-violence-against-women-chapter-1/>.
2. Bartow, Ann. 'Internet Defamation as Profit Center: The Monetization of Online Harassment.' *Harvard Journal of Law and Gender* 32 (2009): 383–429.
3. Bates, Laura. *Everyday Sexism*. London: Simon and Schuster, 2014.
4. Budapest Convention on Cybercrime (Council of Europe Treaty Series No. 185). Opened for signature 23 November 2001; entered into force 1 July 2004.
5. Citron, Danielle Keats. *Hate Crimes in Cyberspace*. Cambridge: Harvard University Press, 2014.
6. Cyber Civil Rights Initiative. '2019 CCRI Survey Results.' Available at: <https://cybercivilrights.org/ccri-2019-survey/>.
7. Dimond, Jill P., Michaelanne Dye, Daphne LaRose, and Amy S. Bruckman. 'Hollaback: The Role of Storytelling Online in a Social Movement Organization.' *CSCW 2013 Proceedings* (2013): 477–490.
8. Dragiewicz, Molly, et al. 'Technology Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms.' *Feminist Media Studies* 18(4) (2018): 609–625.
9. European Institute for Gender Equality (EIGE). 'Gender-Based Cyberviolence: A New Challenge for the EU.' 2017.
10. Freed, Diana, et al. 'A Stalker's Paradise: How Intimate Partner Abusers Exploit Technology.' *ACM CHI Conference Proceedings* (2018): 1–13.
11. Henry, Nicola, Asher Flynn, and Anastasia Powell. 'Online Domestic Violence Reoffending: Perpetrators, Platforms and Accountability.' *Social and Legal Studies* 30(2) (2021): 215–236.
12. Hinduja, Sameer, and Justin W. Patchin. 'Bullying, Cyberbullying, and Suicide.' *Archives of Suicide Research* 14(3) (2010): 206–221.
13. Information Technology Act, 2000 (India), as amended by the Information Technology (Amendment) Act, 2008.
14. Indian Penal Code, 1860, as amended by the Criminal Law (Amendment) Act, 2013.
15. Jane, Emma Alice. *Misogyny Online: A Short (and Brutish) History*. London: SAGE Publications, 2017.

²³ Bates, Laura, *Everyday Sexism* (London: Simon and Schuster, 2014), Chapter 7.

16. Kaur, Navneet, and Gagandeep Kaur. 'Cybercrimes Against Women in India: A Legal Analysis.' *Journal of Legal Studies* 9(1) (2022): 45–62.
17. Lenhart, Amanda, et al. 'Online Harassment, Digital Abuse, and Cyberstalking in America.' Data and Society Research Institute, 2016.
18. Lievens, Eva. 'Bullying and Sexting in Social Networks: Protecting Minors from Criminal Acts or Safeguarding Minors' Rights?' *Computer Law and Security Review* 30(3) (2014): 251–267.
19. McGlynn, Clare, and Erika Rackley. 'Image-Based Sexual Abuse.' *Oxford Journal of Legal Studies* 37(3) (2017): 534–561.
20. Mantilla, Karla. *Gendertrolling: How Misogyny Went Viral*. Santa Barbara: Praeger, 2015.
21. Nadim, Marjan, and Audun Fladmoe. 'Silencing Women? Gender and Online Harassment.' *Social Science Computer Review* 39(2) (2021): 245–258.
22. National Crime Records Bureau (NCRB). *Crime in India 2022*. New Delhi: Ministry of Home Affairs, 2023.
23. Plan International. 'Free to Be Online? Girls' and Young Women's Experiences of Online Harassment.' 2020.
24. Powell, Anastasia, and Nicola Henry. 'Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law.' *Social and Legal Studies* 26(4) (2017): 397–416.
25. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (Supreme Court of India).
26. Slane, Andrea. 'Sexting and the Law in Canada.' *Canadian Journal of Human Sexuality* 22(3) (2013): 117–122.
27. United Nations General Assembly. *Report of the Special Rapporteur on Violence Against Women, Its Causes and Consequences*. UN Doc. A/HRC/38/47, 2018.
28. United Nations Office on Drugs and Crime (UNODC). 'Cybercrime and Gender-Based Violence.' 2021.
29. Vera-Gray, Fiona. 'Men's Stranger Intrusions: Rethinking Street Harassment.' *Women's Studies International Forum* 65 (2017): 9–17.
30. World Economic Forum. *Global Gender Gap Report 2022*. Geneva: WEF, 2022.