WOMEN'S STUDIES CENTRE

Jesus and Mary College
University of Delhi

RESEARCH PROJECT

2020-21

Cyber-bullying, Cyber-stalking and Sexism: A Case Study of Women Students of Delhi University

Prepared by:

Grace Xess, 2nd year, B.A. (Hons) Sociology

Pawni Khurana, 2nd year, B.Sc. Mathematics

Shaiviee Sharma, 2nd year, B.A. (Hons) History

Simran Rai, 2nd year, B.A. (Hons) English

Kriti Sarin, 1st year, B.A. (Hons) Political Science

Shambhavi Mishra, 1st year, B.A. (Hons) Political Science

Project Mentored by:

Dr. Maya John, Convenor, Women's Studies Centre, JMC

Ms. Aneesha Puri, Staff Advisor, Women's Studies Centre, JMC

ACKNOWLEDGEMENTS

***Grace*:** I would like to express my deep and sincere gratitude to our advisor, Dr. Maya John. Her immense guidance and support were the key factors that helped us complete this remarkable project. Her dynamism, vision and motivation, deeply inspired the team throughout the project. The team is extremely grateful to her and to Ms. Aneesha Puri for the countless number of ways in which they inspired the team throughout.

I would like to thank Ms. Gayatri Ahuja for being an exceptional team leader. She led the team with enthusiasm and passion. Her inputs and efforts carried the team to a successful completion of the project. Special thanks to our president, Dhwani Jaisingh, her support to the team kept us motivated throughout the project.

I would also like to thank the research team. It was an enriching experience to work with these driven and hardworking women. The team put in extensive work and displayed a lot of empathy towards other team members especially during these difficult times.

***

***Simran*:** From my first year in College, I wished to work with Dr. Maya John. Having seen her working for various events in the Women's Studies Center, her progressive spirit and knowledge, I have often felt intrigued. She has been a guide and source of inspiration throughout the project.

With her careful observations and continuous pursuit of improvement, Ms. Aneesha Puri enriched my skillset and refined my critical thinking capacity. She kept us going through the most difficult turns in the project with her constant closeness with each one of us.

My contributions would have been incomplete without the persistent words of encouragement from our Research Head Ms. Gayatri Ahuja. The entire WSC Research team, our President (2020-21) Ms. Dhwani Jaisingh, our Vice President (2020-21) Ms. Riya Arora made the whole journey and experience memorable with immeasurable joyous moments.

My team was the closest people with whom I shared this project. We kept working together and growing as a team. I am extremely grateful for their friendly support and compassionate guidance throughout the project.

***

Shambhavi: This project would not have been possible without the continuous support and guidance of several individuals. I would like to thank our Convenor, Dr Maya John, who has been a constant source of guidance throughout the duration of this project. She has assisted us with her valuable insights and motivated us to bring out the best in our project. I would also like to thank Ms. Aneesha Puri, who has been a pillar of support throughout the project and has helped us whenever we have countered problems with our research. It is because of her constant guidance that the research project has been successfully completed.

I would like to express my gratitude towards Ms. Gayatri Ahuja, the head of our research cell, whose tireless patience and enthusiasm has motivated all of us constantly. She has been a source of inspiration for us. I would also like to thank Ms. Dhwani Jaisingh (President), and Ms. Riya Arora (Vice President), the office-bearers of WSC 2020-21.

I am immensely grateful to all the members of the team who have been a part of this project. The contribution of each and every member has been very valuable. Finally, I would like to thank WSC and Jesus and Mary College for providing us with an opportunity to undertake research on this issue of importance.

***

Shaivee: I would like to express my sincere gratitude towards our advisor Dr. Maya John whose constant motivation, guidance and support were integral to the fruition of this project. She inspired us in innumerable ways to work with utmost zeal and passion. I would also like to extend my gratitude to Ms. Aneesha Puri whose observations and valuable insights helped us in overcoming the problems we faced in the course of the project.

I am immensely thankful to Ms Gayatri Ahuja, the head of the research cell, who led the team with immense patience and whose hard work was inspirational. I would also like to thank Ms. Dhwani Jaisingh (President) and Ms. Riya Arora (Vice President), the office-bearers of the WSC for the academic session 2020-21 who made the entire experience a pleasant one.

Lastly, I would like to thank the members of my team who displayed kindness and compassion and worked to the best of their abilities amidst extremely challenging times. The process of working on the project fostered growth and advanced learning.

***

Kriti: I would like to extend my gratitude towards the Women's Studies Centre for giving me the opportunity to be part of the research team and this project. I would also like to thank our convener, Dr. Maya John. It has been great to hear her valuable insights and her immense knowledge about various issues. She has been an inspiration to me and I cannot wait to learn more from her.

Ms. Aneesha Puri has guided us through every step and made sure the project turned out well. She has helped us understand what is expected of our paper and helped us achieve it. She was also very easy to approach and always catered to our doubts.

I would also like to thank our research cell head, Ms. Gayatri Ahuja, for supporting and encouraging us, and for leading this amazing team. I thank the WSC Officeholders for 2020-21, Ms. Dhwani Jaisingh (President) and Ms. Riya Arora (Vice-President) for making my first-year experience with the WSC so memorable.

Lastly, I would like to thank the rest of the team for their efforts in the paper and for supporting and understanding each other's obligations through the devastating second wave. It was amazing working with all of them.

***

Pawni: Blessed to work with the best, I would like to extend my sincere gratitude to our Convenor, Dr. Maya John for guiding, mentoring, and helping us from the very birth of the project. From helping us with our resources and conducting doubt sessions it has been a beautiful journey to work with Dr. Maya John.

I would like to extend my warm gratitude to Ms. Aneesha Puri for clearing our doubts, sitting with us and discussing every detail in-depth, and directing our paper whenever we tend to lose our focus. Her dedication and commitment have to lead to the success of this paper.

I am immensely thankful to Ms. Gayatri Ahuja for believing in me and providing me with such a great opportunity and topic to work with. She has always been an inspiration and a motivating hand when I faced any challenges.

My heartfelt gratitude to Ms. Dhwani Jaisingh (President) and Ms. Riya Arora (Vice-President) for letting me be a part of such motivating and inspiring women.

Lastly, I would like to thank all of my team members for staying through the thick and thin, understanding and encouraging each one of us to bring the best to the table. I have personally learned a lot from the project and am immensely grateful to be a part of it. The project could not have been successful if all of these individuals would not have motivated and supported each other in these tough and critical times.

***

Table of Contents

A Note from the Project Mentors

The Women's Studies Centre (WSC) purports to deploy an intersectional approach to affirm solidarity with all those engaged in the struggle for equality and democratic rights in a world marked by growing structural inequalities. Any understanding of society, both at the level of common sense as well as at the level of traditional academic discourses involves a discussion on the series of socio-cultural, economic and political factors that interact with each other to enable and hinder the participation of different sections of society, thereby making the experiential dimension of different groups in the decision-making that determines their lives, a very complex and layered phenomenon.

Carrying forward our legacy of critical engagement with different facets of society and taking cognizance of the unprecedented times we have been plunged into, owing to the pandemic, this academic year (2020-21), we have expanded and diversified our research endeavours. The increasing reliance on digital spaces both for professional obligations and leisure, have opened the Pandora's box for novel forms of safety concerns for women and marginalized groups of society, while the traditional hierarchies of class, caste, gender and race lurk in the background and manifest themselves in insidious forms. Taking this as our point of departure, the WSC launched a project to trace the trajectory of young women's experiences in the cyberspace so as to examine the loopholes in the existing constitutional safeguards that have rendered women vulnerable to cyber-crimes.

The patriarchal institutions and their multiple materializations have resuscitated themselves to cater to the transitioning realities owing to the cyber revolution. Consequently, cyber-bullying and cyber-stalking have unfortunately become very ubiquitous. In this project, we argue the need for counter-measures with an even more nuanced understanding to oppose these new forms of social injustices. The project is rooted in documenting the experiences of young women who are grappling with digital spaces and assess their awareness about the existing cyber laws and grievance redressal bodies and the efficacy of the same. There is also an attempt to understand the pitfalls associated with the cultivation of culture that results in overt surveillance of digital spaces by government agencies.

This project has been conceptualised and executed during the pandemic when all pedagogical interventions had shifted to the online mode. It bears testimony to the diligence and sincerity of the student researchers who worked tirelessly to collect data and analyse it for a more comprehensive understanding about the gendered nature of participation in the cyber space. This also, once again, goes on to reinstate that technology can be harnessed for bringing positive social changes and we can and should aspire to make the cyber world a safe space for everyone.

Dr. Maya John
Convenor
Women's Studies Centre, &
Assistant Professor
Department of History
Jesus and Mary College

Ms. Aneesha Puri
Staff Advisor
Women's Studies Centre, &
Assistant Professor
Department of English
Jesus and Mary College

Introduction: Defining Cyber-stalking and Cyber-bullying

Combining with various indices of inequalities along the lines of class, caste, race, oppressed nationalities, discriminated sexualities, minority status, etc., gender-based crimes against women have seen a continuous rise in contemporaneous times. In recent times, these crimes have taken a new turn. Perpetrators have found a new way to harass, stalk, abuse, blackmail, and molest women while sitting comfortably in the luxury of their homes. This form of harassment is online and has been facilitated by the constantly evolving digital and communication technology. In real terms, we are witnessing the growing accessibility of such technology in the hands of those who cannot use it responsibly, which in turn, is coalescing with deepening gender inequalities; in particular, the intensifying commodification of women by the mainstream capitalist media.

While we can be grateful to the internet for bringing about ease in communication in human lives, women have suffered the adverse consequences of the very same. These crimes are known as cyber-crimes because they are facilitated by the internet and information technology, and in short, occur in what is known as 'cyberspace'. One of the peculiar features of gender-based cyber-crimes is the lack of usual evidence required to identify a criminal, and the fact that many women refrain from filing formal complaints or informing authorities due to fear of almost immediate and widespread personal defamation. This has exposed women to cyber-defamation and sexual harassment, with predators evolving new ways to use anything on the internet against a woman.

Despite constitutional safeguards against various atrocities, women often fall prey to injustice and oppression. Perpetrators are known to the women victims, and at times, are also unknown persons. Consequently, cyber violence is *not* always limited to unknown people sitting behind their laptops, stalking women, and approaching them with fake identities, but also to close relations/acquaintances. Many women who refuse to share their accounts and passwords with their spouses or boyfriends go onto become victims of such online harassment when they fall-out with such partners. Such circumstances typically entail ex-partners who seek

to exploit women by blackmailing, gaslighting,[1] and even posting their private pictures on internet sites in the bid to take revenge.

While most cyber-crimes go unreported, those that are reported are treated quite callously by authorities. Usually, the authorities either do not consider these offenses grave enough to be taken seriously or find new and innovative ways to pin the burden of the offense on the victim herself. Major reasons for this laxity include the lack of awareness in society with regard to cyber-crimes, the engrained patriarchal functioning of society, and the visible lack of proper infrastructure to detect or combat these crimes.

With the expansion of internet services, more and more people have at least one internet connection in their own homes. Others have easy access to cyber cafes and educational institutions that help fulfil their need for access to the internet. While this level of access is certainly a revolution, it has not come without innumerable problems. Cyberspace has become an instrument for offenders to victimize women, who are the most vulnerable targets on the internet after children. Even though the internet is a fairly new invention, it has seen an unparalleled growth rate. Recent data of 2019 to 2021 shows that, across the world, anywhere between 4.13 billion to 4.66 billion people have access to internet services in one form or the other (Johnson 2021).

The surge in internet access has been accompanied by a proportionate surge in online harassment. Evidently, the world is witnessing upcoming innovations that compromise personal data and the safety of the user. For example, there has been an increase in the popularity of chat rooms, which are online messaging mediums. These chat rooms have gained a notorious reputation for making private data vulnerable to hacking by criminals. Such chat rooms are also hotbeds for harassment and stalking of women users. Likewise, other forms of social media platforms are also infamous due to several complaints of morphing, stalking, threatening, and blackmailing. For instance, Celina Jaitley, a Bollywood actress, filed two complaints with the Mumbai Police, alleging that her pictures had been morphed by a website to promote lingerie products (*Indian Express* 2009).

There are various types of cyber-crimes. Most of the time, these are often interlinked with each other. The most common crime is *cyber-stalking*. Cyber-stalking is so widespread

[1] According to the *Cambridge Dictionary*, 'gaslighting' is the action of tricking or controlling someone by making them believe things that are not true, especially by suggesting that they may be mentally ill.

that most people are unaware that it is an offense. Cyber-stalking is defined as the use of the internet or any other electronic means to harass an individual. It is usually committed with the intention of intimidating the victim and extracting benefits from him/her. These benefits may amount to sexual favours, extortion, etc. Most women have faced cyber-stalking in one form or the other through websites, online chat forums, emails, etc.

Cyber defamation is another form of crime that includes posting defamatory content about someone on the internet or sending defamatory messages on email or on personal chat. Email spoofing is third kind of cyber-crime that is conducted under the garb of a fake identity, making it difficult for the victim to ascertain who the person is. Email spoofing has become so common that now it is difficult to even establish whether the email has been sent by someone you might know or a fake ID. It is usually followed by blackmailing, extortion, or misuse of personal data.

Cyber morphing and cyber pornography often go hand in hand. Cyber pornography is defined as the graphic, sexually explicit subordination of females that is degrading or abusive to the victim, and most importantly, committed without their consent. Often it is linked with morphing, where photographs are taken from personal accounts and then morphed for the purpose of pornography, blackmailing, or humiliation. Meanwhile, cyber hacking involves hacking into the social media accounts of targeted persons and accessing their personal information such as data, details, pictures, etc, and later misusing such information for different negative purposes. Apart from these, cyber victimization encompasses cyber-bullying, cheating, phishing, domestic violence via *cyber flame*,[2] impersonation, blackmailing, etc.

Bullying remains the most common form of abuse experienced by people. For the longest time, our society has paid little heed to bullying as a form of abuse, and many are often seen dismissing it as a way of "fun teasing". However lately, there has been some realization of the fact that it can traumatize the victim and may result in irreparable emotional damage. While identifying bullies in physical spaces is easy for everyone, doing the same in cyberspace is not something all of us are equipped with. Cyber-bullying refers to bullying or harassment of any kind which is inflicted through electronic or communication devices such as computers, mobile phones, laptops, and usually involves text messages, phone calls, e-mails, instant

[2] Flaming is the act of posting or sending offensive messages over the Internet. These messages, called "flames," may be posted within online discussion forums or newsgroups, or sent via e-mail or instant messaging programs. https://techterms.com/definition/flaming.

messages, social media platforms, or chat rooms. It ranges from the posting of hurtful words, derogatory comments, fake information on public forums or blogs to threats to rape or kill.

The most frequently used definition of cyber-bullying is "an aggressive, intentional act or behavior that is carried out by a group or an individual, using electronic forms of contact, repeatedly and overtime against a victim who cannot easily defend him or herself" (Smith 2013). Importantly, bullying traditionally involves a stronger person asserting his or her superiority over a weaker person to his or her advantage. With the advent of the internet, it has also become possible for a person with *neither* superior physical strength *nor* financial clout to bully another. In many cases of cyber-bullying, the bully uses a fake identity and the anonymity offered by the internet to stay away from the clutches of the victim and the law.

While the state agencies need to strengthen the legal system; enhance the promptness of police work so as to mitigate cyber-crimes; and improve infrastructure that can quickly track and combat these offenses, it is also imperative for individuals to be vigilant and precautious. It is important to take certain steps like verifying identities before sharing any sensitive personal information in cyberspace, not sharing private data or passwords with anyone, and most importantly, not staying silent about being subjected to a cyber-crime.

Research objectives and methodology

This project is geared toward collecting and analysing the experiences of university-going students, especially women in the age group of 18 to 25 years, with respect to cyber-stalking and cyber-bullying. Our sampling was based on a prevailing assessment that cyber-bullying and cyber-stalking are most profound among *younger* age groups, as they are heavy consumers of social media. This has also made them susceptible to mental health problems like depression. (Landstedt & Persson 2014, 393). The project is working with the premise that cyber-stalking and cyber-bullying are rapidly growing phenomena, that a bulk of the victims are women students, and that official reporting of the matter is often minimal. In this light, an online survey has been widely circulated among Delhi University students to corroborate such trends.[3]

A total of 204 responses were received, ranging from undergraduate to postgraduate women students (18-25 years) of the University. The primary objective was to assess typical

[3] Due the disruptions posed by the COVID-19 pandemic, the shift to online classes and this year's April-May lockdown, our methodology was restricted to the online circulation of our survey, although we had hoped to circulate it in-person, followed by more detailed interaction with a cross-section of respondents.

forms of cyber harassment in such an age group, their knowledge of the pre-existing cyber laws, and the efficacy of the same among the youth. In order to ensure confidentiality and maintain ethical integrity, participants were made to fill a consent form before the actual survey. It was ensured that they understood the objective of the survey and the basic definition of cyber-stalking.

As part of the analysis of experiences recorded, the team seeks to comment on the existing legislation against cyber-stalking and cyber-bullying and, furthermore, on the question of accessibility of legal redress available to young women. While looking to highlight and contribute to ongoing discussions on model practices for online interactions, this project also seeks to explore the debate on the importance of stronger laws balanced against the pitfalls associated with draconian surveillance of digital spaces by government bodies.

Key Cyber Laws and their Fault-lines

The legal ammunition: an overview

Cyber-crimes in India are addressed majorly by two laws, the Indian Penal Code, 1860 and the Information Technology Act, 2000. The laws are complementary when it comes to functioning and both have been amended several times over the years to incorporate provisions that pertain to the changing needs of the society. Significantly, the National Commission for Women (NCW) found out that while the laws provide a legal remedy to victims of cyber-crimes, there were considerable loopholes and gaps in the laws that posed a challenge when it came to tackling crimes or hearing cases. The Indian Penal Code, 1860 (IPC), neither defines bullying nor punishes it as an offense. However, various provisions of the IPC and the Information Technology Act, 2000 (IT Act) can be used to fight cyber-bullies. To address these issues, the NCW organized the 2nd consultation to review laws on cyber-crimes. It was important to make the existing laws more gender-sensitive, while at the same time identifying and correcting inadequacies in the present framework that hindered the justice delivery mechanism.

Under the IPC, Section 354A and Section 292, deal with offenses related to cyber morphing, pornography, cyber defamation, etc. These offenses carry a punishment of up to 3 years, accompanied by a hefty fine. Provisions on sharing images or videos of a woman engaged in an intimate act, without their knowledge and consent are covered under Section 354C. The term of serving a sentence can go up to 7 years if the accused is convicted for a second time. Section 354D states that cyber-stalking is an act of sexual harassment and the offender can face jail term ranging 3-5 years coupled with a fine as per the IPC.

There have been a few landmark cases that have charted out the position of women in the cyber world. The Manish Kathuria case was the first cyber-stalking case that was tried in India. The perpetrator stalked a woman called Ritu Kohli through online sources and then abused her by sending vulgar and obscene messages. Another landmark case was the Karan Girotra case where the accused had drugged and sexually assaulted a woman. Then, he harassed the victim by sending her pictures of the assault and blackmailed her to circulate the images if the woman did not marry him. A complaint was lodged under Section 66A of the IT Act. President Pranab Mukherjee's daughter Sharmistha was harassed by a man who posted

sexually explicit messages on her Facebook page, following which she filed a complaint in the cyber cell of the Delhi police.

In the case of *State of West Bengal v. Animesh Boxi*[4] , the accused took possession of some private and intimate photographs of the victim by hacking into her phone, blackmailed her by threatening to upload the stolen pictures and videos on the internet, and subsequently uploaded her private pictures and intimate videos onto an obscene website. The District Court of West Bengal convicted the accused under sections 354A, 354C, 354D, 509 of IPC, and sections 66C and 66E of the IT Act. The court held that the offense u/s 354D of the IPC is proved as the victim was not only stalked online but also suffered from 'virtual rape' every time a user of the openly accessible global website viewed the video. The court commented that deterrence was one of the prime considerations for convicting the accused and an inadequate sentence would do more harm than justice, as it would undermine public confidence in the seriousness of the issue.

Indian laws such as the Indian Penal Code and the IT Act have provisions on various cyber offenses such as Section 67 that stipulates the period of conviction if the accused has been proved guilty of circulating images and videos without the victim's free will and consent. It is important to take preventive measures such as not sharing private data with someone on the internet, not communicate with unknown people, approach online acquaintances with cautiousness, be aware of the recent technological developments, save all forms of communication as proof, and finally, contact the local police or cyber-crime authorities and provide them with every information that will help in catching the offender.

Women and cyber-crime

It is important to note that women are one of the most vulnerable sections of society. India has been witnessing a steadfast rise in cyber-crimes all over the country. Many forms of cyber-stalking have also resulted in rape and murder. Despite this, we tend to treat cyber-crime very leniently since there is a perceived notion that cyber-crimes do not amount to physical threats or that, cyber-stalking will not turn into stalking. We also subconsciously practice victim blaming, questioning the woman to somehow justify why she became a victim. In 2013, Justice J.S. Varma Committee had played a great role in the incorporation of various criminal laws such as 354A, 354B, 354C, and 354D which deals with stalking of women. Extradition

[4] *State of West Bengal v. Animesh Boxi*, GR No. 1587 of 2017.

of stalkers who are not citizens of India continues to be a major issue, while at the same time, the laws are exclusive of male and trans victims of cyber-stalking.

As mentioned earlier, cyber-stalking remains one of the most common cyber-crimes faced by women. The NCW in its legal module on 'Gender Sensitization and Legal Awareness Programme'[4] defines cyber-stalking as following:

> Stalkers are strengthened by the anonymity the internet offers. He may be on the other side of the earth, or a next-door neighbour or a near relative!' It involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat rooms frequented by the victim, constantly bombarding the victim with emails, etc. In general, the stalker intends to cause emotional distress and has no legitimate purpose to his communications.

In other words, cyber-stalking is an extension of the physical form of stalking, committed over the internet, through e-mail, or other electronic communication devices and can take different forms including slander, defamation, and threats. It includes, *inter alia*, the following:

- Sending threatening or obscene messages, posts, or emails;
- Stealing a person's identity online and circulating false information with the intent to humiliate or harass;
- Tracing the location of a person through illegal means;
- Uploading obscene pictures;
- Posting derogatory remarks online with the intent to harass.

The Press release on 'Digital Exploitation of Children', by the Ministry of Women and Child Development states that sections 354A and 354D of the IPC provides punishment for cyber-bullying and cyber-stalking against women. Importantly, cyber-stalking of women was recognized as an offense, after the insertion of section 354D in the IPC through the Criminal Law (Amendment) Act, 2013. Section 354D of IPC defines stalking as a condition involving the following (emphasis added):

> *Any man who*: *1) follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or 2) monitors the use by a woman of the internet, email, or any other form of electronic communication, commits the offense of stalking:*
>
> *Provided that such conduct shall not amount to stalking if the man who pursued it proves that*
>
> *i) it was pursued for the purpose of preventing or detecting crime and the man accused of stalking had been entrusted with the responsibility of prevention and detection of crime by the state;*

ii) it was pursued under any law or to comply with any condition or requirement imposed by any person under any law;

iii) in particular circumstances such conduct was reasonable and justified.

The language of Section 354D of IPC, thus, makes it clear that the section penalizes both the offense of offline and online stalking, without discriminating on the basis of presence or absence of the 'cyber' component. However, sub-section (2) fails to clarify the way the victim can be said to be 'monitored' or 'watched', or what constitutes such acts.

The lacunae

Anita Gurumurthy and Niveditha Menon (2009) aptly highlight the following loopholes in the present IT Act, 2000. These loopholes not only raise necessary concern about the existing legislation, but also indicate the dire need for policies and new laws which would help women, albeit without curbing their privacy or online freedom. They rightly argue that the IT Act was made to facilitate the booming e-commerce industry in India. The laws under this are specifically made for the e-commerce industry, and are consequently least concerned with individual safety and cyber-crimes unleashed on individuals and vulnerable age groups. For example, the IT Act does *not* talk about consent and free will. Therefore, if women engage online in sexual acts of their own choice, they can still be booked under the IT Act because the consent of the parties involved is not considered. The only provision that considers consent is the matter of images taken via phone. Such a void in the law also relates to the ownership of images. For example, if a woman has consented to her pictures being taken but does not want them to be publicized, the rules of ownership, and how can these rules of ownership be legislated and enforced, repeatedly surface as debatable issues. Such issues are especially relevant in the context of the queer movement in India, wherein the Internet has provided a feasible and vibrant space for sexual minorities to communicate and network (Gurmurthy and Menon 2009).

Furthermore, women who are victims of cyber-crime are usually characterized as 'emotionally weak' or 'unstable', with paternalistic policies and patriarchal-oriented institutions conveniently seeking to regulate women's choices in the name of safety and protection. There is then an urgent need to build a wider dialogue around the interface of technology with prevailing culture, institutions of family and marriage, varied sexualities, body politics, privacy, and the freedom of expression. In other words, we need policy interventions to protect and further women's rights, protect individual privacy in the effort to curb exploitation and tyranny, as well as enable highest possible transparency in governmental

regulation of cyberspace. Evidently, the protection of women's rights to information and communication emphasizes the need to balance concerns of self-expression with concerns of protection from exploitation.

While there is no doubt that policies are needed to address online violence, the boundaries of state involvement in effecting such protection becomes critical. While the governmental agencies should be able to swiftly prosecute those engaged in violence against women, a blanket right to surveillance in general, i.e., without constituting rational parameters that sync with constitutional safeguards and without ushering in other judicial and police reforms, is a measure that is likely to infringe on women's privacy. Notably then, the state's responsibility to intervene and prosecute violence when it happens online should not become an excuse for authoritarian surveillance over the Internet. Thus, policy approaches need to recognize both women's "public", political rights as well as their "private", individual rights, especially in the context of violence against women (Gurumurthy and Menon 2009).

It is imperative to note that while cyber-crimes are a relatively new issue, they have been proliferating at a staggering rate. The lockdown has seen an increase in cyber-crimes all over the world, most of the victims being female. It is also important to address the issue of data privacy since personal information such as bank details, photographs, etc are often used to blackmail the victims and coerce them into doing activities against their will.

The increase in cyber-crimes and our justice delivery mechanism also highlights the callousness of several authorities while dealing with cyber-stalking cases. Complaints of stalking, bullying, or harassment are rarely entertained or taken seriously since there is no presumed threat in these cases. At the same time, it is also important to point out the casual victim shaming a woman encounters when she registers a cyber-stalking complaint. She is blamed for talking to or trusting someone, for not complaining early, for not taking adequate measures to protect herself, etc. This results in distrust in the courts and police stations, stopping women from filing cases against their cyber-stalkers, which in turn boosts the confidence of the perpetrators.

We must acknowledge the fact that there is a lot that we need to cover a lot of ground in order to stop these crimes. Even though India is comparatively well developed in terms of technology, we are unable to support software that can swiftly track or detect these crimes. The need of the moment is to create inclusive, holistic and nuanced laws in the information

technology sector, mainly because the cyberspace grants a user the privilege of anonymity, which is not an easy feature to regulate. Moreover, the trend of victim shaming and blaming must immediately stop as it is highly counterproductive and circumvents concrete solution-building, addressal of institutional laxity, and provides perpetrators with considerable advantage in an otherwise patriarchal public domain. Justice delivery mechanisms in the country need to be reformed, and this can only be achieved when there is a systemic change in the way we view women, the multitude of sexualities in existence, and concrete human rights.

A Case Study of Women Students of Delhi University

Social media usage and its impact on well-being

The increase in use of technology has led to a massive rise in the number of people who have access to social media. In 2020 alone, there were 3.96 billion people actively using social media across the world; a significant increase of 10.9 per cent from 2019 (Kemp 2020). Within this user base, a large proportion are youth.

From our survey pool of 204 participants in the age bracket of 18 to 25 years, 90.7 per cent of the respondents answered in affirmative when they were asked if they use social media actively, with 62.7 per cent people being moderate social media users (128 respondents), 24 per cent being heavy social media users, and just 13.2 per cent people indicating that they use social media sparingly. In our sample, Instagram is the social media application (app) used by around 88.7 per cent of the respondents, with just a few using other apps like Twitter, Facebook, Snapchat, etc.

Harassment in all forms significantly impacts the well-being of young women. Our survey revealed that most women had experienced *online* harassment in one form or another. These included getting repetitive calls, accounts getting hacked, getting impersonated online, inappropriate texts/slut-shaming messages, among others. Noticeably, the use of social media platforms has impacted the mental health and well-being of the respondents in many ways due to hacking, online abuse and threats, as reported by 31.4 per cent; the receipt of repetitive calls as shared by 40.7 per cent; the receipt of sexist or personal comments that were considered inappropriate by 17.6 per cent; etc.

One of the most commonly reported forms of online abuse is texts from fake accounts. About 141 respondents (69.1 per cent) admitted that they had received inappropriate messages from random accounts. Majority of these are seen in Instagram DMs (Direct Message) requests, including messages displaying nudity or asking for sexual favours. One respondent even reported that she was incessantly approached for her number on LinkedIn (a strictly professional platform), asking to discuss a 'work proposal' that could not be done on text. Such accounts are a testament to the fact that most of the online harassment that women face is

explicitly sexist in nature. Furthermore, those who identify as queer, reported harassment on the basis of their identity and getting misgendered.

The case of fake accounts

Social media has definitely made a really special place in our lives and we do not fail to make it a part of our daily routine. As social beings, we tend to share pictures, videos and stories of the happy moments in our everyday life. In this vein, our life is not really private and we do not shy away from sharing many little details with the world. However, amongst all the positive likes and comments, the content that goes online is not always as safe as the privacy policies claim them to be. Bullies and haters do find a way to harass and spread hate on such content. When we asked our 204 respondents whether or not they felt safe uploading their pictures on social media, a majority, i.e., 128 respondents (62.7 per cent) responded 'Yes', while 76 respondents (37.3 per cent) responded 'No'. These responses clearly highlight the doubt and fear in the minds of many people while they upload pictures on their social media handles.

It is a common practice now to find social media users stalk a celebrity, an ex-'best friend', or even make a fake account to view someone's account who has may has blocked them online. On the surface these are pretty harmless actions wherein we have no intentions to cause harm or distress to anyone on social media and in real life. The problem occurs when actions of online stalking, catfishing,[5] making multiple fake accounts, etc. are done for the sole purpose of causing mental or physical harm to somebody. According to a study conducted in 2018 by Ghost Data, shockingly almost 95 million Instagram accounts are automated (Kalfaoglu and Akyon 2019). Turning to official data, we find that there were 8,379 cases of r-crime which related to sexual harassment or exploitation reported across India in 2019 as per data released by the National Crime Records Bureau. These crimes included cyber-stalking, harassment, pornography, defamation, morphing, etc. A total of 289 cases of fake profiles under the IT Act were filed in the same year.

When we asked our respondents if they ever come across accounts that seemed to be fake or were made for the purpose of stalking people online, a majority, i.e., 191 respondents (93.6 per cent) responded 'Yes' while only 13 respondents (6.4 per cent) responded 'No'. In addition to this, out of 204 respondents, 141 respondents (69.1 per cent) have received inappropriate messages from random accounts. Together these numbers from our sample

[5] The process of luring someone into a relationship by means of a fictional online persona.

corroborate a disturbing ground reality; namely, how acts of stalking, multiple fake accounts, etc. are being regularly used with malicious intentions like harassment, bullying, and inflicting mental or physical pain on someone.

Victim-perpetrator relationship

In cases of cyber-crimes against women, the dynamics of the victim– perpetrator relationship has much to reveal about widespread, every-day gendered realities that make many women fall prey to online harassment. In our survey, we attempted to study this relationship. In a question that asked the respondents to determine whether their cyber harassers were known to them, our survey revealed that 82.1 per cent of the respondents were not familiar with the identities of their offenders while the remaining 17.9% respondents were familiar with their offenders. This in itself indicates the high levels of impunity with which the average male in our society can seek out a woman to harass.

In a subsequent follow-up question, respondents were asked to choose from a set of given options to throw light on the deeper details of the victim–perpetrator relationship. The question asked them to define the familiarity they had with their perpetrators. The options provided to the respondents were the following: i) not known to you, ii) work-related contact, iii) know indirectly to you, i.e., through someone else, iv) well-known to you and v) not applicable. The responses revealed that while 27.9 per cent of the respondents opted for 'not applicable', a significant number, i.e., 53.4 per cent of our respondents did *not* know their perpetrators from before. On the other hand, 10.8 per cent respondents reported knowing their perpetrators indirectly through another person, 6.9 per cent claimed that the perpetrators were well-known to them, and for one per cent of our respondents, the perpetrators were work-related contacts. The variety in the responses received indicates that in cases of cyber-crimes, a broad generic pattern cannot be easily applied to the victim–perpetrator relationship. This relationship can vary from that of contacts well-known to the victim, i.e., close kins like spouses to co-workers to friends, friends of friends, distant acquaintances of relatives to absolute strangers. However, what could be determined was that a majority of the respondents did not know their offenders, indicating that the models of cyber-crimes have their peculiarities. Such crimes were completely technology-driven, operating in the cyberspace, as opposed to several forms of 'traditional' offline harassment wherein victims and perpetrators tendentially know each other due to their shared physical settings. While not established as the absolute

truth, an ignorance of the identity of cyber harassers among victims can be a result of the opportunity to hide, transform, or assume identities which cyberspace enables for perpetrators.

This apart, it is also important to recognize a visible trend in cyber-crimes which occur at the hands of male acquaintances/kin. Although in our sample, fewer respondents claimed to have known their perpetrators than those who did not, it is not at all uncommon for women to fall prey to former partners, spurned acquaintances and overzealous, patriarchal male kin members. In our society that is shaped by patriarchal values and norms, women stand at the receiving ends of extreme cases of cyber-crimes. Attaching dominant roles to men and submissive ones to women is a societal trend that ensures the perpetration of cyber-crimes like cyber-stalking wherein male offenders who are close kins of the victims, 'keep watch' on the victims (females), which they assume is 'their duty' as 'determined' by their gender.

Psychological impact

One major reason why devoting attention to cyber-crimes against women achieves increased importance with every passing year is because the impact that cyberspace has on our society widens every year as more people gain access to it. The pervasive negative effects of cyber-crimes against women reveal how they trigger multiple undesirable emotions and reactions. Our survey studied the trends related to some of these effects. The respondents were asked to identify the nature of the impacts that cases of cyber-stalking and cyber-bullying left on them. While 28.9 per cent of our respondents reported being shocked and embarrassed, 38.9 per cent of them were angered and felt like retaliating. This 38.9 per cent represented the most widespread response that the survey revealed. However, ours is a society that seldom ever gives women the chance to manifest their anger and retaliate, leading to many women suppressing such emotions.

Moving on, 32.4 per cent of the respondents reported being scared, 17.2 per cent identified feeling hurt and isolated, 19.6 per cent reported being depressed and very anxious. while 2.5 per cent shared that they felt suicidal. In response to this question, 29.9 per cent opted for 'not applicable' whole 12.7 per cent identified feeling indifferent to the cyber harassment. When generalized, these statistics reveal that barring a small population, a significant percentage of women are likely to be faced with negative emotions as a result of cyber-crimes. The psychological impacts of such crimes can by no means be ignored. The impact can be severe enough to even push the victims towards suicide, which is an extremely serious matter.

In a follow up question, the respondents were asked whether they took cyber awareness or counselling sessions post the incident. While 27.5 per cent of them opted for 'not applicable', a total of only 4.9 per cent respondents reportedly took such sessions. Notably then, a majority, i.e., 67.6 per cent of our respondents did not avail of any counselling. This data points to the significant gap between women and their access to mental health infrastructure and cyber awareness mechanisms. More than one-third of the respondents did not access these and while this might be reflective of their individual decisions, these decisions do not remain isolated from societal realities. The access to mental health infrastructure and cyber awareness mechanisms remains limited and hence difficult to achieve for women. Such facilities are extremely expensive, and there is a stigma generally attached to both counselling services as well as to reportage of sexual harassment such that and women, owing to their submissive stature in society, often find it difficult to address their concerns in the first place.

Data privacy and redressal mechanisms

Data privacy and protection are some of the most important concerns today. In recent times, there have been cases of 'data leaks', the most recent one being via Facebook, which put personal data of about 533 million users to threat (Sen & Bagchi 2021). With digitization in almost every domain, the government now has control over most of our personal data. In addition, there are very few or no safeguards to secure that data from unauthorized platforms. The Data Protection Bill, 2019 has also raised serious concerns about how the government can access our data, to protect the national interest. Apps like Instagram and Facebook have their own set of privacy policies and terms. However, not everyone pays attention to them. Interestingly, 24 per cent of our respondents did not read the privacy policy before signing up for such apps. On the other hand, awareness about complaint mechanisms such as reporting was comparatively higher.

To protect women, there are personal safety apps in place that alert a pre-fixed emergency contact about their whereabouts or apps that can check identities when someone calls you. Some of these are TrueCaller, Himmat Plus, Durga Shakti, as well as inbuilt SOS features in iOS and Android phones. Of our total respondents, 85 per cent had a fair idea about these apps/features. However, this is not enough. There are still loopholes or poorly formed rules that make it possible for cyber-stalkers to easily get access to a woman's private information. Social media apps do have their complaint mechanisms which are sometimes quite effective. Other times, women's pictures are misused or spammed with derogatory comments.

Significantly, a fair number of respondents emphasized that women posting anything on social media should not be anyone's business, and asking them to not post 'revealing' pictures is blatant victim-blaming. Instead, there should be stricter and faster action against perpetrators. This clearly suggests that Facebook's reporting feature needs to be reworked and catered more organically to women's safety. Furthermore, 20.6 per cent of women who took the survey felt that the security measures provided by dating apps and social networking apps are ineffective against cyber-crimes.

Social media applications and their safety net

Out of 204 responses that we received, the majority, i.e., 94 respondents, reported partial awareness about the security features available on social networking sites. It was only a meagre number of 26 respondents who responded that they were fully aware of such features. Further, a majority of our respondents were not sure of any concrete steps taken by these applications/sites when a complaint was registered with them. This ignorance and lack of confidence about the reporting mechanisms also result in the wider trend of under reporting of the abuse faced by women online. It appears that a heavy majority does not report the crime, and, that women users tend to shut themselves off the online spaces when untoward incidents of cyber-stalking and bullying unfold. This further goes on to aggravate the paranoia women experience vis-à-vis their safety concerns. Consequently, women not only lose the opportunity to learn and grow in the online spaces, but these spaces also remain male-dominated spaces where women can be bullied by anonymous male users with impunity, i.e., without suffering any repercussions.

Additionally, our responses also indicate that social media applications need to ramp up their interface with women users so as to better acquaint them with their complaint registration mechanisms. Moreover, well-advertised and user-friendly complaint mechanisms in social media applications, followed by swift action or complaint resolution, are essential to the enabling of women users to report formal complaints; thereby, keeping a check on online sexism and cyber-bullying.

Response of the police

A few responses accentuated the fact that many women hesitate to resort to redressal mechanisms like lodging an official complaint with the police. Those who did, on the other hand, did not find it helpful.

The personal experiences of victims are indeed aggravated due to the indifference of the police. The police remain difficult to access in the first place and expecting indifference and ignorance from them remains the pervasive commonsensical thought. The answers to the related questions posed in our survey reinforce this belief. Upon being asked whether they contacted the police or not, 54.4 perc cent of our respondents answered that this didn't apply to them, while 42.1 per cent reported that they did *not* contact the police. Only a small 3.5 per cent reported contacting the police. In a subsequent question that noted the nature of the response received from the police, the percentage of respondents who did not get a response from the police and who received a delayed response stood at one per cent each, while those who received a prompt response formed a small 2.9 per cent of the total respondents. On corroborating data received in some of the previous questions, we found that a large number of respondents who reported facing cyber-crimes never reported them to the police. A particular response on a long answer question helped us gain more perspective on why the help of the authorities is often not sought in cases of cyber harassment. The response read:

> It is embarrassing and burdensome to reach out to the authority for any help. For their response is never against the perpetrator but the victim. I'd rather forget than get involved any further.[6]

While a small number of respondents, i.e., three respondents, mentioned receiving an adequate response from the police, the aforementioned response is overall reflective of irresponsible behaviour from the authorities.

Legal mechanisms

Legal ammunitions to provide protection against cyber-crimes like cyber-bullying and cyber-stalking were put in place several years ago. However, the dissemination of knowledge regarding the constitutional provisions, and more specifically, regarding the clauses of various laws has not been adequate. Of the total respondents who took the survey, 53.4 per cent were aware that privacy is a fundamental right, while 38.2 per cent were only moderately aware of the same. Notably, the percentage of respondents having knowledge of the clauses of the IT Act, various provisions of which can be used to fight cyber-bullies, was comparatively less and stood at 23 per cent claiming awareness of it and 45.1 per cent respondents claiming only moderate awareness of this law. This indicates an expected higher knowledge of rights in

[6] Our survey provided the respondents the option of specifying if they would like to stay anonymous, and whether we could quote their experiences or not. This particular respondent agreed to the latter but on the condition of anonymity.

general as against knowledge of important laws to defend fundamental rights. When asked if they were aware of existing cyber-stalking and cyber-bullying laws in India, while 80.9 per cent respondents indicated that they were *not* aware about any, and only 19.1 per cent indicated that they were aware. The follow up question asking the respondents to name some of those laws was answered by only 15 respondents out of our sample size of 204, with many reporting to have read about/studied such laws but having forgotten them. Some of the responses received in this regard were as follows:

> 1) The Indian Penal Code, 1860 (IPC), neither defines bullying nor punishes it as an offence. However, various provisions of the IPC and the Information Technology Act, 2000 (IT Act) can be used to fight cyber bullies.
>
> 2) The Press release on 'Digital Exploitation of Children', by the Ministry of Women and Child Development states that the sections 354A and 354D of the IPC provides punishment for cyber-bullying and cyber-stalking against women. Cyber-stalking of women was recognised as an offence, subsequent to the insertion of section 354D in the IPC through the Criminal Law (Amendment) Act, 2013.

The coherent picture that emerged from our sample was one of ignorance regarding the laws as more that four-fifths of the respondents were visibly unaware of the law. One of the obvious requirements is, thus, to make the laws known as their existence on paper alone does not solve the problems of the victims. This also indicates the need for compulsory education/awareness-building in school and college curriculums regarding the same.

The instances of cyber-crimes against women are higher as the ongoing pandemic has pushed more people towards accessing the internet, and consequently, the cyberspace. In this light, obnoxiously low levels of legal knowledge about infringements of rights in cyberspace, low reporting of complaints of cyber-crimes, and lax police action stick out as huge problems. Interim solutions like awareness-building about online forms of harassment and about mechanisms of complaint registration and redressal; introduction of pending police reforms; plugging of gaps in existing legislation; etc. are desperately needed in today's context.

Conclusion

While callous action by governmental authorities aggravates women's problems in accessing whatever assistance is available to deal with instances of cyber-crimes, it is also important to build and contribute towards the much-needed counter-culture that destigmatizes women's privacy on and off social media. We can hope that with conscious awareness-building and a stronger and more widespread gender justice movement, our society will be able to disassociate

itself from the vicious culture of victim blaming, that more efficacious laws are enforced, and that the authorities are pushed into being more sensitive and accessible.

Here, we would like to point to a news article in the *Economic Times* (December 2020), which reported that "Cyber experts have suggested a proper grievance redressal mechanism, that is user-friendly, multilingual and known to all to tackle cyber-crimes faced by women, according to the NCW." In its fifth law review consultation on cyber-crimes against women, the NCW pointed out that its panel of experts from the cyber world emphasized the need for better implementation of the existing laws. They also pointed to the pivotal role of including laws related to cyber-crimes in school curriculums that would help make children aware of these crimes at young ages, and to the urgency of sensitization and capacity building of police personnel so as to adequately equip them with the skills and sensitivity to act on cyber-crimes as well as to apply related laws in a comprehensive manner.

Data privacy has emerged as one major concern to address while dealing with issues of cyber-crimes against women, who are seen as soft targets online. While many corrective measures necessitate reforms by the state, social media applications must themselves strengthen their privacy, safety and redressal mechanisms. Moreover, advocacy is likely to build a more aware community of internet users, especially women, whose enhanced general awareness regarding cyber-crimes and the law is also pivotal to eradicate such harassment. University organisations like Women's Studies Centres/Women's Development Cells, Internal Complaints Committees/Gender-Sensitization Cells, etc., that have a pervasive influence among students today, can be seen addressing these important issues, and therefore, are taking the first steps in the direction of prevention of such harassment through awareness-building and facilitating prompt action against perpetrators. These platforms help destigmatize the issue of women's mental health in a context of rampant harassment and its fallouts; actively discourage victim blaming; and spread required awareness about cyber safety – all of which are crucial to ensuring the online safety of college-going women.

Procedural Information and Advice

How to complain about cyber stalking?

- Firstly, a written complaint must be registered in the cyber cell of her jurisdiction. If there are no cyber cell facilities in a particular place, then the person can file a complaint in the local police station.
- If the local police do not file a First Information Report (F.I.R.) or accept a written complaint, then the person can also directly approach the Commissioner or Judicial Magistrate of the city.
- If a woman approaches the police station with an accusation of cyber-stalking, she is allowed legal aid to help her file a case.
- The statement of the victim always be taken down in private. The cyber police station has women police constables who can help the complainant to file a complaint.

Suggestions for safeguards

- Protect digital devices like smartphones, tablets, laptops, and other oft-used computers with passwords / finger lock, and change these on a regular interval so that no one can hack it.
- Always remember to logout from any website or application when you are not using it.
- Always use secured sites for browsing information and making of payments. Never enter your phone number, address and other information on an unsecured website.
- Never mention personal information and family information on social media, and always make your account private, keeping the data available only to close friends.
- Never add unknown persons to your social media account to increase the number of followers.
- Never update your current location or places that you are visiting on social media. Remove events you are about to attend in the future.
- Try to avoid the use of other people's phone or laptop for your personal use, and if you do so, proceed to remove the browsing history as well to logout.
- If you find anything wrong/suspicious, take the screenshots and lodge a formal complaint as soon as possible with the application/customer care/your institution/the police.

Some digital gyaan on how to be safe online

1. *Keeping a low profile*
    - Avoid putting out personal details such as an address, phone numbers, intimate photos, and other details that reveal real-time information such as your location or who you are with, etc.
    - For individuals who need online platforms for self-promotion or business-related activities can restrict and tone down on the details they post online.

- Use nicknames on platforms like Twitter or Instagram which are not related to your professional sphere. Avoid accepting requests or direct messages from unknown people or strangers, do check before accepting anything on your account's activity.
- It sometimes gets impossible to hide personal information on some platforms like Online Dating, but these are the sites that are home to online attackers and sometimes you may even end up chatting with a potential cyberstalker. The best way to this is to be careful and do thorough background research of the platform you are using and preferably use reputed sites.

2. *Update your software*

- It does not come off as a first measure to be cyber safe but keeping software up to date is crucial while staying cyber safe as it prevents information leaks. Many updates ensure to patch security vulnerabilities and help to keep the information safe.
- It is extremely important for phones because they contain valuable details like bank accounts, email accounts and can even help attackers track your location.

3. *Hide your IP address*

Many of the applications and services we consume reveal our IP address to the person we are communicating with and this address is directly linked to our personal data. For example, our IP address is directly linked to our internet bill and our credit card with which we make the payment. This is useful information for the stalkers to find the credit card data and trace our home address. To prevent your IP address, you can:

- Use VPN (Virtual Private Network) which helps to hide your real IP address and replaces your current location from the location or country you set it to. It also helps to encrypt your internet traffic keeping it safe from hackers.
- Another alternative to this is to use Tor Browser, which encrypts your internet traffic but be cautious while using it because it may raise red flags for law enforcement agencies because it is commonly used for criminals themselves.
- For getting ultimate anonymity, you can combine Tor and VPN. Using a web proxy or a free VPN service are not the best options to use as they harm your online security more than they help it.

4. *Maintain good digital hygiene*

Digital Hygiene is a new and upcoming term that represents a very crucial topic regarding social networks. Maintaining good digital hygiene helps you to protect yourself from cyber harassment, cyber-bullying, and cyber-stalking. In this regard, it is important to:

- Keep your privacy settings is one of the first steps to clean up your account and prevent it from any hack. At times some platforms let you know who can see your information and who can contact you.
- Another way can be to keep your posts, timelines, stories, message threads and feeds free from negative and unpleasant content to avoid any potential feeling of negativity from others and might have a significant negative emotional impact if you re-read them later.

5. *Avoid disclosing sensitive information*

Apart from putting out information on social media, avoid filling up random questionnaires or submitting applications for coupons that ask for personal data as this increases your chances of getting cyber attacked.

What to do in case you are being cyber-stalked?

- Block the individual who threatens or sends you unpleasant content. Do not hesitate to exercise the powers and access given to you.
- If someone is trying to threaten you, immediately block the individual and then report it to the platform involved, i.e., report it to Facebook, WhatsApp, Instagram, etc. These platforms usually have easy-to-access buttons to quickly report any kind of abusive behaviour.
- There is a possibility that you think that you are rid of the attacker, but they may come back or even pursue more victims.
- Law enforcement agencies are not always equipped with technical tools to protect you from cyber-stalking, but platform moderators usually respond quickly and delete attackers' profiles.
- Report it to the police if you feel their behaviour is illegal and needs to be reported, even if you do not have enough evidence against them for immediate prosecution, the report will be added to the police record and the police can then guide you on how to proceed further.

References

Chapter 1: Introduction

1. Aune, N. M. (2009, December): "Cyberbullying." Retrieved from https://www2.uwstout.edu/content/lib/thesis/2009/2009aunen.pdf

2. Indian Express News Service. (2009): "Celina Jaitley complains to police against website." Retrieved from https://indianexpress.com/article/entertainment/entertainment-others/celina-jaitley-complains-to-police-against-website/.

3. Johnson, Joseph. (2021, April 7): "Global digital population as of January 2021." Retrieved from https://www.statista.com/statistics/617136/digital-population-worldwide/.

4. Landstedt, E. and S. Persson. (2014, June): "Bullying, cyberbullying, and mental health in young people." *Scandinavian Journal of Public Health*, 42, 393-399. Retrieved from https://www.jstor.org/stable/45150813?seq=1#metadata_info_tab_contents

5. Smith, P. K., C. del Barrio and R. S. Tokunaga. (2013): "Definitions of bullying and cyberbullying: How useful are the terms?." In S. Bauman, D. Cross, & J. Walker (Eds.), *Principles of cyberbullying research: Definitions, measures, and methodology*, New York: Routledge/Taylor & Francis Group, pp. 26–40.

Chapter 2: Key Cyber-Laws and Their Faulty Lines

1. Gurumurthy, Anita and Niveditha Menon. (2009, October 3): "Violence against women via cyberspace." *Economic and Political Weekly*, Vol. 44 No. 40. Retrieved from https://www.epw.in/journal/2009/40/commentary/violence-against-women-cyberspace.html

2. Joseph, Vinod and Mitali Jain. (2020, October 1): "Anti-Cyber Bullying laws in India- An Analysis." Retrieved from https://www.mondaq.com/india/crime/989624/anti-cyber-bullying-laws-in-india--an-analysis.

3. Kemp, Simon. (2021, July 21): "More than half of the people on earth now use social media." Retrieved from https://datareportal.com/reports/more-than-half-the-world-now-uses-social-media.

4. Kumar, Lovish and Shivam Jindal. (2019): "Cyber-stalking: technological form of sexual harassment," *International Journal on Emerging Technologies*, Vol.10 No 4, pp. 367-373. Retrieved from https://www.researchgate.net/publication/339140114_Cyber_Stalking_Technological_Form_of_Sexual_Harassment.

5. National Commission for Women. (2020, September): "Newsletter Volume 1, No 248," Retrieved from http://ncw.nic.in/sites/default/files/RMSeptember2020Eng.pdf

6. Singh, Jaspreet. (2015, January): “Violence Against Women in Cyber World: A Special Reference to India,” *International Journal of Advanced Research*, Vol. 4 No 1. Retrieved from https://garph.co.uk/IJARMSS/Jan2015/8.pdf

Chapter 3: A Case Study of Women Students of Delhi University

1. Kalfaoglu, M. E. and F. C. Akyon. (2019): “Instagram fake and automated account detection. *Innovations in Intelligent Systems and Applications Conference*.” Retrieved from https://arxiv.org/pdf/1910.03090.pdf.

2. Pittaro, Michael L. (2007): "Cyber stalking: An Analysis of Online Harassment and Intimidation," *International Journal of Cyber Criminology*, Vol. 1 No 2, pp. 180-197. Retrieved from https://www.cybercrimejournal.com/pittaroijccvol1is2.htm.

3. Saha, Tanaya and Akancha Srivastava. (2014): "Indian women at Risk in the Cyber Space: A Conceptual Model of Reasons of Victimization," *International Journal of Cyber Criminology*, Vol. 8 No 1. Retrieved from http://www.cybercrimejournal.com/sahasrivastavatalijcc2014vol8issue1.pdf.

4. Sen, D. and R. Bagchi. (2021, April 15): “Facebook data leak: How are Indian users affected, and should you worry?.” *Indian Express* Retrieved from https://indianexpress.com/article/explained/facebook-data-leak-explained-7268515/.

5. The Economic Times. (2020, December): "Experts suggest proper grievance redressal mechanism to tackle cybercrimes against women.” Retrieved from https://economictimes.indiatimes.com/news/politics-and-nation/experts-suggest-proper-grievance-redressal-mechanism-to-tackle-cybercrimes-against-women/articleshow/79531395.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

6. Tripwire. (2018, December 5): "What cyberstalking is and how to prevent it.” Retrieved from https://www.tripwire.com/state-of-security/security-awareness/what-cyberstalking-prevent/

Appendix – 1

Cyber-bullying, Cyber-stalking and Sexism: A Case Study of Women Students of Delhi University

Online questionnaire circulated by the Research Cell of the Women's Studies Centre, Jesus and Mary College, University of Delhi.

1. CONSENT FORM:

Dear participant,

The Women's Studies Centre of Jesus and Mary College (JMC), University of Delhi is pursuing a research project which is geared toward collecting and analysing the experiences of university-going students, particularly women, with respect to cyber-stalking and cyber-bullying. Our research team involves bonafide students of JMC who are members of the college Women's Studies Centre. We are mentored by the faculty members of the college. The college Women's Studies Centre is a UGC-funded centre. We utilize the findings of our research projects for our annual magazine *Jigyasa*; for publication on suitable, socially relevant blogs that generate awareness on rampant social problems; and for official student-research conferences.

We are working with the premise that cyberstalking and cyberbullying are a rapidly growing phenomena, that a bulk of victims are women students, and that official reporting of the matter is often minimal.
We are conducting this online survey to:
(i) test the above-mentioned general observations,
(ii) draw out specific trends with respect to who the usual perpetrators and victims can be,
(iii) gain insights on the typical patterns of such harassment in the age group of 18-25 years (i.e. undergraduate students to young research scholars of DU).
(iv) assess the knowledge/awareness that digitally aware college-going youth have about the laws, and their access to existing legal remedies against cyber-stalking and cyber-bullying.

This online survey is a voluntary exercise. If you wish to participate, please specify your response to the following clauses / provisions of this research:

(i) You are participating in this online survey out of your own will?

YES /NO

(ii) You have understood the purpose of the research for which the questionnaire is being shared with you

YES /NO

(iii) You agree to allow the research team to use your responses for streamlining key arguments about cyber-stalking and to make recommendations for needed action?
YES/NO

(iv) You are comfortable with your name being used, if need be, to make a point/argument in the final report?
Yes. use my name as it is.
No
Opt for name change in instances where experiences need to be quoted

(v) You are comfortable if the Research Team reaches out to you for a further interaction on your experience/s?
YES/NO

** Before proceeding to answer the questionnaire, would you like to familiarize yourself with basic definitions of cyber-bullying and cyber-stalking?
NO/YES

DEFINITION: Cyber-bullying refers to a host of hostile activities such as:
Gossip: posting or sending cruel gossip to damage a person's reputation and relationships with others;
Exclusion: deliberately excluding someone from an online group;
Impersonation: breaking into someone's online account and sending messages or making posts that will cause embarrassment or damage to the person's reputation and affect their relationships with others;
Harassment: repeatedly posting or sending offensive, rude, and insulting messages or posts;
Cyberstalking: posting or sending unwanted or intimidating messages, which may include threats;
Flaming: online fights where scornful and offensive messages are posted on websites, forums, or blogs;
Outing and Trickery: tricking someone into revealing secrets or embarrassing information, which is then shared online.

I. PERSONAL DETAILS:

(i) Age:
(ii) Gender:
1. Male

2. Female

3. Other

(iii) Occupation:

(iv) Name (optional if you have selected NO in the consent form above):

(v) Contact number and email ID (optional):

(vi) Course and year of studies at Delhi University:

(vii) Are you an undergraduate student, postgraduate student or research scholar?

II. EXPERIENCE WITH SOCIAL MEDIA PLATFORMS

(i) Are you an Active user of Social Media platforms?

1. YES

2. NO

(ii) On a scale of 1 to 3, please rate your usage of digital/social media platform

1: Little (E.g.: you use less than two social media platforms and do not check these on a daily basis)

2: Moderate (E.g.: You use two or more social media platforms and check them / post on them on a daily basis)

3: Heavy user (E.g.: Due to work or habit, you tend to use several social media platforms and are checking/posting a couple of times in the day)

(iii) What Social Networking sites do you use the most?

1. Instagram

2. Facebook

3. Twitter

4. Snapchat

(iv) Do you feel safe uploading your pictures on social media?

YES/NO

(v) Have you ever come across accounts that seem to be fake/made for the purpose of stalking people online?

YES/NO

III. IMPACT OF SOCIAL MEDIA AND ITS TRANSACTION ON YOUR WELL-BEING

(i) Have you ever faced the following? (You can select more than 1)

a) Received abusive or threatening calls, emails, messages or posts

b) Received repetitive calls

c) Discovered false information or rumours being spread about yourself through social media

d) Been impersonated in emails or messages

e) Been tracked or monitored through online stalking apps

f) Had your social media accounts/computer hacked and personal information/pictures revealed.

g) Sexist trolling

h) Been tagged to / received sexist, objectionable posts

i) Any other inappropriate behavior (name it)

j) Haven't faced any

(ii) Are there any social media websites/Apps where you got harassed?

1. Facebook
2. Whatsapp
3. TikTok
4. Instagram
5. Tinder
6. Twitter
7. Youtube
8. If other, please specify _____
9. Not applicable

(iii) Have you ever received inappropriate messages from random accounts?

YES/NO

(iv) If you have selected 'yes' above then please provide some details about the nature of the incident.

(v) How would you exactly identify your online harassment? (You can select more than one response).

1. Sexist in nature
2. Offensive along other lines such as commenting on your caste, economic status, community affiliation, regional background, family background, etc.
3. Offensive along the lines of commenting on your alternative sexuality
4. An outright financial crime
5. Not applicable

(vi) Were the person/s harassing you on social media, known to you?

1. Yes
2. No
3. Not applicable

(vii) How would you define the familiarity between you and your perpetrator?

1. Not known to you
2. Work-related contact
3. Known indirectly to you, i.e., through someone else
4. Well-known to you
5. Not applicable

(viii) How have you been impacted by instances of cyber-stalking and cyber-bullying? (You can select more than one option).

1. Shocked and embarrassed
2. Angered and felt like retaliating
3. Scared
4. Hurt and isolated
5. Depressed and very anxious
6. Suicidal
7. Indifferent
8. Not applicable

(ix). Have you taken any cyber awareness or counselling or session after the incident?

1. Yes
2. No
3. Not applicable

IV. CYBER-BULLYING AND REDRESSAL MECHANISMS

(i) Do you feel the digital space should be optimized through intrusion by law making authorities?

1. Yes
2. No

(ii) Do you read the privacy policy of the application before signing into it?

1. Yes
2. No
3. Sometimes

(iii) Are you aware of any personal safety apps and alerting systems?

1. Yes
2. No

If Yes. Please mention_____

(iv) Are you aware about security features available on social networking sites and the process of reporting?

1. Not at all
2. Somewhat aware
3.Aware
4. Fully aware

(v) Women are often warned against putting pictures that can be misused. Do you think this is a correct / adequate prevention tool?

1. Yes
2. No
3. Maybe

(Please explain your response: _____)

(vi) Are you aware that Privacy is a Fundamental Right?

1. Little Aware but not sure of all the clauses
2. Not aware
3. Aware

(vii) Are you aware of the Information Technology (IT) Act, 2000?

1. Little Aware but not sure of all the clauses
2. Not aware
3. Aware

(viii) Do you know of any laws in India which are used to address cyber-stalking and cyber-bullying?

1. No
2. Yes

*If yes, then name some laws: _____

(ix) Are you aware about the cyber-crime reporting website launched by the Ministry of Home affairs, Govt. of India?

1. Yes
2. No

(x) Do you think that cyber security should be introduced in the curriculum of schools and colleges?

1. Yes
2. No

(xi) Do you think social media applications like Facebook, Instagram, Twitter and Dating Apps provide adequate help when a case of cybercrimes is reported via their application?

1. Yes
2. No
3. Maybe
4. Sometimes

V. PERSONAL EXPERIENCE WITH GRIEVANCE REDRESSAL

(i) If your private content were misused, did you reach out to the Content Provider?

1. If Yes, what was the response?
2. No
3. Not applicable

(ii) Did you contact the Police?

1. Yes

2. No

3. Not applicable

(iii) How did you approach the Police?

1. FIR at Police Station

2. Reported Online

3. Used some other redressal mechanism (please specify)

4. Not applicable

(iv) Please select the kind of response you received from the Police:

1. Did not hear back from them

2. Delayed response, requiring you to pursue the matter with them regularly

3. Prompt response, guidance and action

4. Not applicable

(v) If you filed a police complaint, what is the status of your complaint:

(vii) Any other Comments: