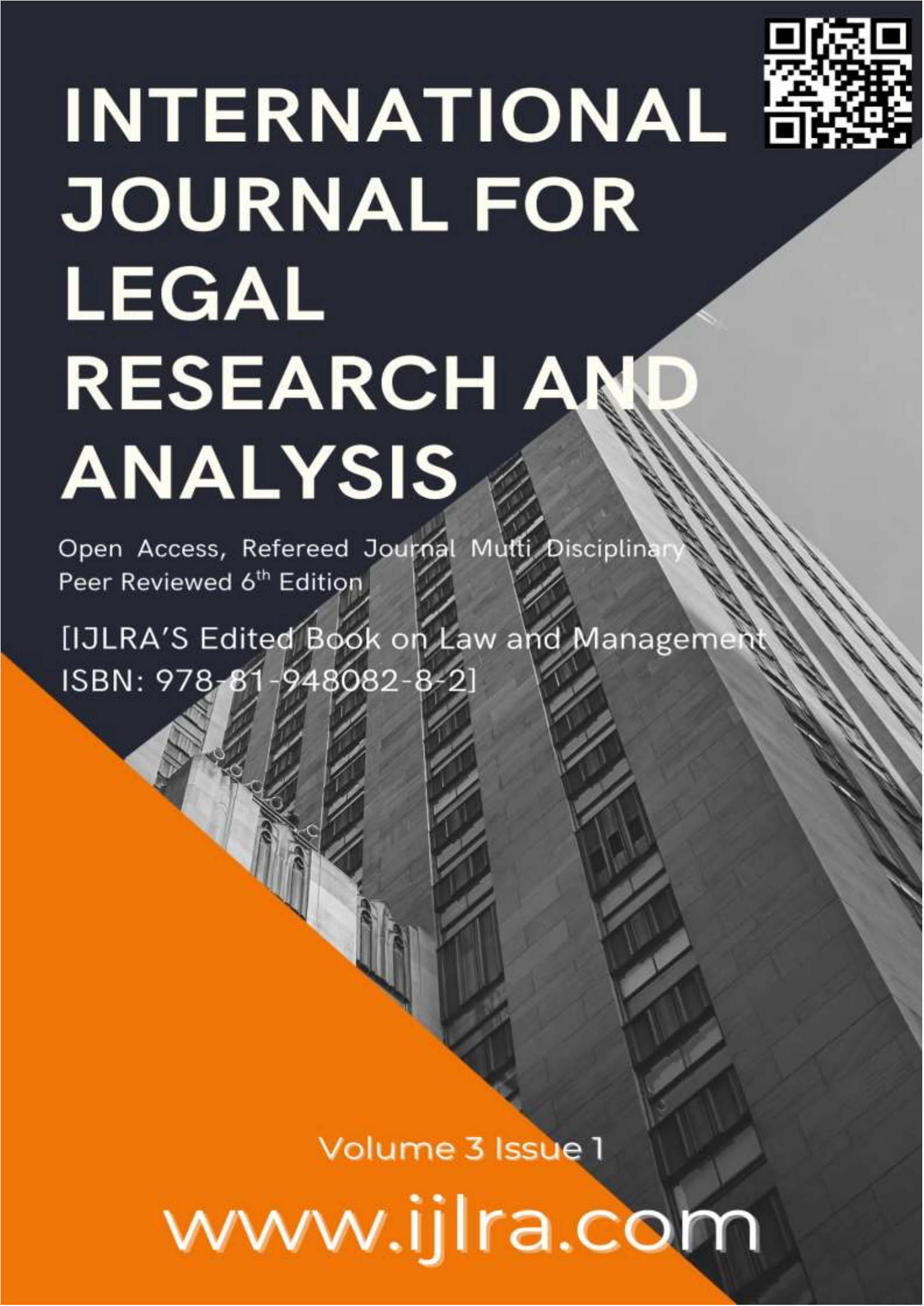
INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed 6th Edition

[IJLRA'S Edited Book on Law and Management
ISBN: 978-81-948082-8-2]

Volume 3 Issue 1

www.ijlra.com

 ISBN: 978-81-948082-8-2

DISCLAIMER

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

 ISBN: 978-81-948082-8-2

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC - NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISBN: 978-81-948082-8-2

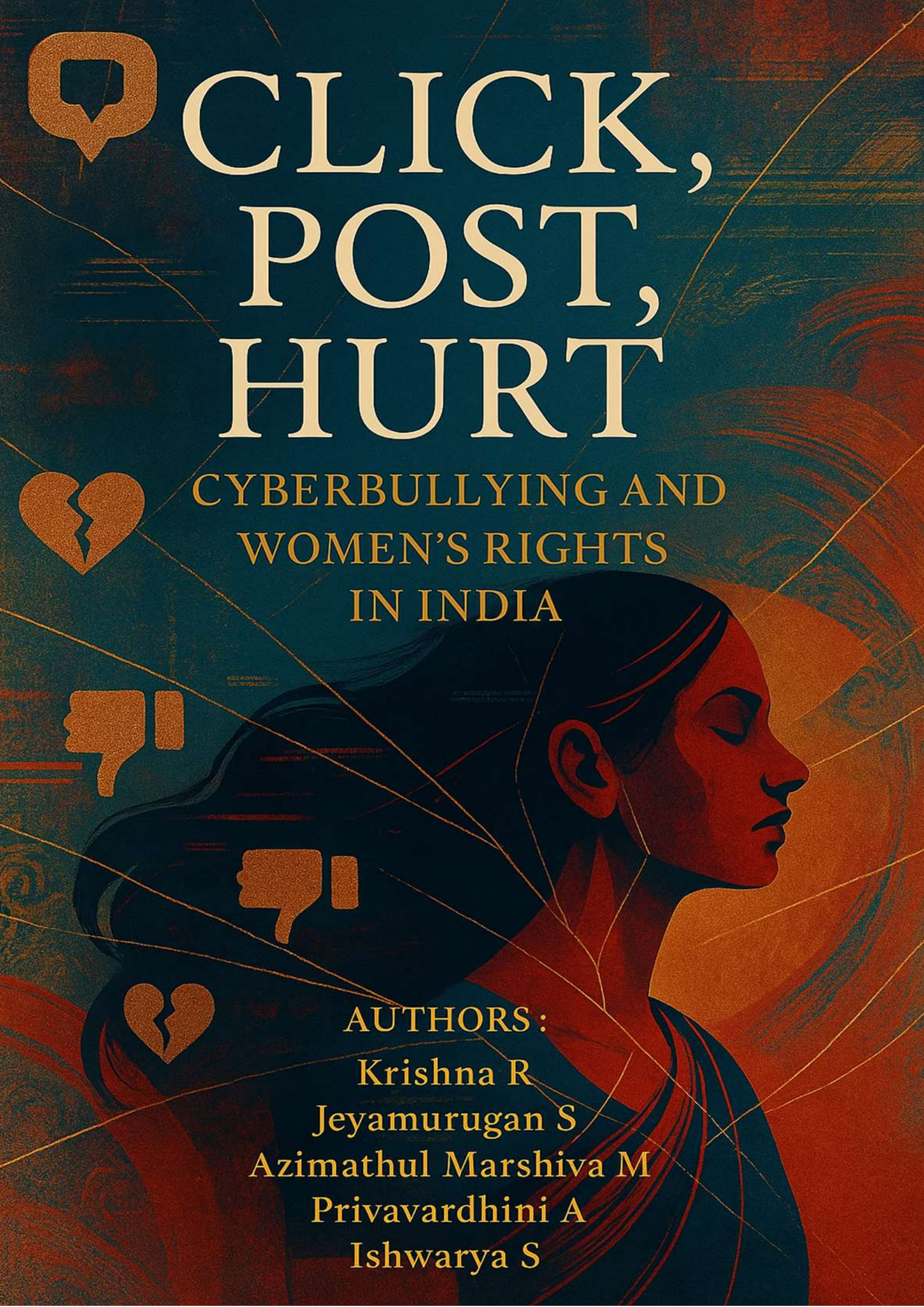
ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISBN

978-81-948082-7-5 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISBN 978-81-948082-7-5 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

CLICK, POST, HURT

CYBERBULLYING AND WOMEN'S RIGHTS IN INDIA



AUTHORS :

Krishna R

Jeyamurugan S

Azimathul Marshiva M

Privavardhini A

Ishwarya S

 ISBN: 978-81-948082-8-2

CYBERBULLYING AND WOMEN'S RIGHT IN INDIA

AUTHORS:

Chapter 1:

Krishna R

Sathyabama school of law

Assistant Professor of law

Chapter 2:

Azimathul Marshiya M

Assistant Professor of law

Bharath institute of law -BIHER

Chapter 3:

Jeyamurugan S

Assistant professor of law Bharath institute of law

Chapter 4:

Privavardhini A

Assistant Professor

Bharath institute of law

Chapter 5:

Ishwarya S

Assistant Professor

Bharath institute of law

 ISBN: 978-81-948082-8-2

PREFACE

There is an unnerving undercurrent in the huge digital world, where ideas come together, dissent is expressed, and communities are formed: women are disproportionately singled out, silenced, and shamed. For many, what ought to have been a place of empowerment and independence has turned into a battleground for psychological trauma, abuse, and harassment. The urgency of that reality is what inspired this work. Cloaked by anonymity and emboldened by quiet, it is a modest but forceful attempt to address the gendered violence that festers in our encrypted texts and social media feeds.

This book's journey started as a moral reckoning as much as a legal investigation. It became more and more obvious that the existing legal, sociological, and technological systems are insufficient with each message shared by a survivor, trial that failed because of antiquated legal standards, and social media post that sparked a storm of misogyny. They are reactive, disjointed, and frequently unaware of the multiple hazards women experience on the internet. Reform alone is not enough; reimagining is also required.

This book, which is organized into six in-depth parts, starts by analysing the gendered aspects of cyberbullying and placing it in a socio-legal and psychological framework. It investigates the shortcomings of our existing legal system and challenges the social conditioning that encourages victim blame.

The book goes beyond criticism to trace the function of social media networks. It poses difficult queries regarding corporate responsibility, algorithmic collusion, and the role of the judiciary in interpretation. Comparative analysis of international legal systems also highlights the ways in which other democracies face comparable challenges, providing guidance and inspiration for India's future.

Every woman who chose to speak online despite being told she shouldn't be honoured in this preamble. I hope you keep raising your voice and that the law eventually learns to pay attention.

 ISBN: 978-81-948082-8-2

CONTENTS

 ISBN: 978-81-948082-8-2

CHAPTER - IV

COMPARATIVE ANALYSIS OF INTERNATIONAL LEGAL SYSTEMS

CHAPTER - V

GENDER, TECHNOLOGY, AND LAW: NAVIGATING CYBERBULLYING LAWS IN INDIA

 ISBN: 978-81-948082-8-2

CHAPTER - VI

TOWARDS GENDER-INCLUSIVE ONLINE JUSTICE

ABBREVIATIONS

AIR	All India Reporter
CDA	Communication Decency Act
Cr.P.c	Criminal Procedure Code
CCIC	The Cyber Crime Investigating Cell
CCU	Cyber Crime Unit
EU	European Union
GDPR	General Data Protection Regulation
IT ACT	Information Technology Act
ITAA	Information Technology Amended Act
IPC	Indian Penal Code
ICCPR	International Covenant on Civil and Political Rights
ICJ	International Court of Justice
ISPAI	Internet Service Providers Association of India
ISPs	Internet Service Providers
POCSO	Protection of Children from Sexual Offences
SCC	Supreme Court Cases
Sec.	Section
SMS	Short Message Service
SNSs	Social Networking Sites
TRAI	Telecom Regulatory Authority of India
UK	United Kingdom
US	United States of America
V.	versus
VAWA	Violence Against Women Reauthorization Act
WWW	World wide web

LIST OF CASES

LIST OF STATUTES

INDIAN LEGISLATIONS

The information technology act, 2000

The Indian penal code, 1860

The information technology (intermediary guidelines and digital media ethics code) rules, 2021

Protection of children from sexual offences (POCSO) act, 2012

The constitution of india, 1950

INTERNATIONAL LEGISLATIONS

The protection from harassment act 1997

The malicious communications act 1988

The Communications Act 2003

The enhancing online safety act 2015

The harmful digital communications act 2015

Bill C-13, the Protecting Canadians from Online Crime Act

CHAPTER-I

INTRODUCTION

"Cyberbullying, when aimed at women, often reflects deeper societal misogyny. It's not just about silencing women online; it's about undermining their very presence and voice in the public sphere." - Catharine A. MacKinnon,

In the evolving landscape of digital communication, social media platforms have become arenas where societal norms and conflicts are both reflected and reinforced. As these platforms increasingly serve as conduits for interpersonal interactions, they also become spaces where inequalities and abuses manifest uniquely. This book explores the complex interplay between gender, technology, and law, focusing particularly on how these dimensions converge in the context of cyberbullying and victim blaming of women on social media. The prevalence of online harassment targeted at women raises critical questions about the efficacy of legal frameworks, the responsibilities of technology providers, and the societal underpinnings of gender-based violence in digital spaces.

Understanding the Gendered Dimensions of Cyberbullying

Cyberbullying, defined as the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature, has emerged as a profound issue in the age of the internet. Research indicates that women are disproportionately targeted by cyberbullying and are more likely to experience severe emotional impacts as a result. The gendered nature of cyberbullying on social media platforms reveals a disturbing overlap with traditional forms of gender-based violence. This connection suggests that old societal prejudices and power imbalances are being repackaged into new technological forms.

The combination of caste, gender, and communal identities in India exacerbates the type of cyberbullying that women face. Online harassment, such as caste-based slurs, sexual threats, and altered photos, is frequently more severe for Dalit women, female journalists, activists, and public figures. In India, Muslim women leaders were subjected to 94% more abusive tweets than their counterparts, according to 2020 Amnesty International research on online harassment of female politicians. It is crucial to use an intersectional perspective when analyzing online harassment because, as this concerning figure shows, gendered cyberbullying is not a separate problem but rather is entwined with larger systems of marginalization.

Social media's anonymity and reach give offenders more confidence, and because of lax enforcement and a lack of reporting of cybercrimes, they frequently act without consequence.

The common advice given to women to "keep quiet" or "ignore" violence reinforces social norms that put the onus of safety on the victim rather than the attacker. Persistent online harassment can also cause psychological trauma that can result in long-term mental health problems, self-censorship, and retreat from public debate. In addition to limiting women's internet engagement, this illustrates how cyberbullying stifles democratic liberties. In the current digital era, a gender-sensitive perspective is consequently essential to comprehending the nature and purpose of cyberbullying.

Challenges in the Legal Framework Addressing Digital Harassment

From a legal perspective, the challenge lies in the adaptation of existing laws to encompass the new modalities of harassment facilitated by digital technologies. The effectiveness of these legal frameworks in protecting women from online harassment is often hampered by the transnational nature of the internet, jurisdictional limitations, and the rapid evolution of technology which outpaces legislative responses. The legal discourse surrounding cyberbullying and victim blaming on social media is marked by a call for more robust legal protections that are nuanced enough to address the specific needs and contexts of women.

Technology companies that operate social media platforms play a pivotal role in this ecosystem. The design and policy decisions of these platforms can either curb or exacerbate the incidence of cyberbullying. The responsibility of these companies in implementing and enforcing policies that protect users from harassment is crucial. However, there is an ongoing debate about the extent to which these companies should be held liable for the actions of their users and the effectiveness of their interventions.

There is no stand-alone law in India that specifically addresses cyberbullying as a distinct and gendered type of digital violence, despite the fact that several statutes make online obscenity, sexual harassment, and defamation crimes. This legislative gap frequently leads to poor enforcement outcomes, misclassification of online abuse, and uncertainty among investigative agencies. Even while several previous laws that attempted to control online speech were overturned due to their possible abuse and excessive scope, their removal has created a big gap in the fight against targeted digital harassment, particularly against women.

The absence of gender understanding and digital sensitivity among law enforcement officials further widens this disparity. Because of social stigma, insufficient police reaction, and worries about being accused or embarrassed, victims of cyberbullying especially women frequently refuse to report such crimes. Implementation is still uneven even though several committees have suggested training and reforms for officials handling gender-based violence.

Furthermore, effective investigation and prompt remedy are frequently hampered by a lack of data privacy standards, protracted procedural delays, and a lack of cooperation by international digital platforms. What is desperately needed is a thorough legal response that is adapted to the changing landscape of cyberbullying a framework that is socially conscious, technologically aware, and legally binding in order to protect women's safety and dignity online.

Societal Attitudes and the Culture of Victim Blaming

Victim blaming, where the victim of a crime or any wrongful act is held entirely or partially responsible for the harm that befell them, is particularly pernicious in the context of cyberbullying. This phenomenon reflects and reinforces broader societal norms that blame women for the harassment they experience, thereby exacerbating the trauma and isolation felt by victims. This book seeks to explore these themes in depth, providing a comprehensive analysis of the intersection of gender, technology, and law in the context of cyberbullying and victim blaming of women on social media. By examining the implications of these interactions, the aim is to contribute to a better understanding of digital harassment and to propose effective strategies for legal and societal reform to protect women online.

Patriarchal attitudes are still ingrained in Indian society, influencing how mistreatment of women is viewed and dealt with both offline and online. The prevailing narrative frequently challenges the victims' decisions rather than denounces the perpetrators when women are the targets of online harassment, particularly when they share intimate photos, voice strong opinions, or discuss political or feminist concerns. Women are supposed to be quiet or avoid public interaction as a way of "avoiding trouble" as a result of this social conditioning that internalizes patriarchal control over their behavior. In addition to discouraging women from using digital platforms, these viewpoints normalize abuse as an inevitable byproduct of being visible.

Such blaming has structural as well as psychological effects. Authorities frequently show skepticism toward women who try to denounce online harassment or seek legal retribution because they view the matter from a moral rather than a legal perspective. The same biases that are shown in cases of physical sexual harassment or assault are often replicated when questions are raised about a victim's attire, behavior, online persona, or past relationships. Because of these institutional prejudices and a lack of gender-sensitization, many women choose to keep quiet rather than seek justice, perpetuating secondary victimization. In addition

to legislative reform, addressing this deeply embedded culture calls for a shift in public perceptions through media portrayal, education, and community awareness initiatives that place the blame entirely on offenders rather than victims.

Rationale for focus on Cyberbullying Against Women

Cyberbullying against women in social media platforms is paramount due to the increasing prevalence and severity of cyberbullying incidents targeting women. Social media has become an integral part of modern communication, offering a platform for individuals to express opinions, share experiences, and connect with others. However, this same platform has also become a breeding ground for cyberbullying, especially against women, who often face gender-specific forms of harassment, including sexual harassment, threats of violence, and defamation. The legal frameworks currently in place have struggled to keep pace with the rapid evolution of technology, leading to significant gaps in addressing and remedying these online behaviors. A focused work on how gender influences the experiences and legal outcomes of cyberbullying cases is crucial. Such research could illuminate the deficiencies in existing laws and the need for tailored policies that protect individuals against gender-specific cyber harassment. Furthermore, examining the social norms and biases that contribute to victim blaming on social media can aid in developing more effective educational and preventive measures. This book seeks to bridge these gaps by providing comprehensive analysis and actionable insights into the confluence of these critical areas, aiming to enhance legal responses and promote a safer, more equitable online environment for women.

Cyberbullying against women on social media platforms is paramount due to several reasons. Firstly, women are disproportionately targeted for cyberbullying, facing harassment, threats, and defamation that can have severe psychological, emotional, and even physical consequences. Understanding the nature and extent of cyberbullying against women is crucial for developing effective prevention and intervention strategies. Secondly, social media platforms play a central role in modern communication and have become virtual spaces where cyberbullying thrives. Investigating how women are targeted on these platforms can inform policies and practices to create safer online environments.

This book aims to uncover the nuanced ways in which legal frameworks can be either empowering or insufficient in addressing the complex issues of cyberbullying and victim blaming. By focusing on women as primary victims within the social media landscape, this research highlights the urgent need for legislative evolution to keep pace with technological advancements. The findings could provide empirical evidence to support more robust legal

protections and contribute to the broader discourse on gender equality in the digital age. Furthermore, it seeks to empower stakeholders, including policymakers, educators, and social media platforms, to implement more effective strategies for prevention and redress, thus fostering a safer online environment for all users.

CHAPTER-II

CYBERBULLYING AGAINST WOMEN IN INDIA

Cyberbullying, a modern-day peril facilitated by digital platforms, has emerged as a critical concern in India, particularly affecting women. This phenomenon extends beyond traditional bullying into the digital space, where harassment, threats, and abuse occur through social media, emails, and messaging apps. The anonymity and reach of the internet magnify the impact of such behaviours, making cyberbullying a pervasive and insidious form of violence against women. In India, the rise of internet users has been accompanied by an increase in cybercrimes, with women often being disproportionate targets. The motivations behind cyberbullying against women are deeply entrenched in societal attitudes towards gender, power dynamics, and cultural norms that sometimes tolerate aggression against women. Cyberbullying can range from sexist remarks and character assassinations to more severe forms such as cyberstalking and identity theft, leaving profound psychological impacts and, in extreme cases, leading to physical harm.

What is Cyberbullying?

Cybercrime refers to criminal activities that are carried out using computers or the internet. It encompasses a wide range of illegal activities, including hacking, phishing, identity theft, fraud, and spreading malware, among others. Cybercrime can target individuals, businesses, or even governments, and it can have serious financial, social, and psychological consequences for victims. On the other hand, cyberbullying specifically refers to the use of electronic communication to bully, harass, or intimidate someone, typically through social media, messaging apps, or other online platforms. Cyberbullying can take many forms, such as sending threatening messages, spreading rumors, sharing embarrassing information, or excluding someone from online groups. It is often targeted at individuals, particularly children and teenagers, and can have devastating effects on their mental health and well-being.

MEANING - The term "cyberbullying" is a compound word derived from "cyber" and "bullying." The prefix "cyber" originates from the Greek word "Kubernetes," meaning "steersman" or "pilot," and was later adapted into Latin as "cybernetes." It eventually found its way into English through the word "cybernetics," coined by mathematician Norbert Wiener in the 1940s to describe the study of communication and control systems in living organisms and machines. In modern usage, "cyber" is commonly associated with computers, the internet, and digital technology, reflecting its evolution from its original meaning to encompass the realm

of electronic communication and virtual environments.

The term "bullying" has roots in the Middle Dutch word "boele," which originally referred to a lover or brother, but later came to mean "brotherly love" or "kindness." Over time, the meaning of "bullying" shifted to denote intimidation, coercion, or harassment, particularly in the context of interpersonal relationships. The modern definition of bullying, as a form of aggressive behavior intended to cause harm or distress to others, emerged in the late 17th century. When combined, "cyber" and "bullying" create a compound word that refers to the use of electronic communication and digital technology to engage in aggressive or harassing behavior towards others. The term "cyberbullying" gained prominence in the late 20th and early 21st centuries with the rise of the internet and social media platforms, reflecting the growing prevalence and impact of online harassment and abuse.

Bill Belsey, a Canadian educator, is credited with coining the term "cyberbullying." It refers to the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature. This form of bullying can occur through various digital platforms such as social media, messaging apps, or online forums. The definition often includes actions that go beyond the limits of normal communication to harm a person's reputation, state of mind, or to humiliate them. Cyberbullying can have serious consequences for the victim's mental health and well-being, making it an important issue to address in today's digital age.[1]

The definition of cyberbullying in Indian law is not clearly established, as there is currently no specific legal framework that comprehensively defines cyberbullying. However, various aspects and behaviors related to cyberbullying can be derived from broader cybercrime legislation and other legal provisions. The absence of a universally accepted definition for cyberbullying, or bullying in general, remains a challenge as "cyberbullying" serves as a broad term encompassing various aggressive behaviours conducted through information and communication technologies. This lack of a standardized definition is recognized as problematic.

Cyber-bullying is defined as a deviant act which is conducted through an electronic device (computer –smartphone-tablet etc.) when the offender according to the FBI's definition is harassing, threatening or intimidating an individual or a group of individuals through these devices (FBI, Cyberbullying Report, 2019).

The Budapest Convention, formally known as the Council of Europe Convention on Cybercrime, is an international treaty designed to address Internet and computer crime by

[1] Ciol Bureau, India lacking laws to curb cyber bullying, (Dec. 9, 2007) http://www.ciol.com/indialackinglaws-curb-cyberbullying/. (Last visited 14,May.2024)

harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. While the Convention primarily focuses on offenses related to cybercrime such as fraud, child pornography, and security breaches, it does not explicitly mention "cyberbullying". However, provisions within the Budapest Convention could potentially apply to acts of cyberbullying if they intersect with other criminal behaviors covered by the treaty. For instance, if cyberbullying involves illegal access to computer systems, data interference, system interference, or the misuse of devices, aspects of the Budapest Convention could be relevant. Additionally, the transnational nature of many cyberbullying incidents could engage the Convention's mechanisms for international cooperation and support[2]

The USA National Crime Prevention Council specified that “Cyber-bullying could be limited to posting rumours or gossips a person in the internet bringing about hatred in other's minds, or it may go to the extent of personally identifying victims and publishing materials severely defaming and humiliating them” (US National Crime Prevention Council, 2017).
While cyberbullying is a form of cybercrime, not all cybercrimes involve bullying behavior. Cybercrimes can be financially motivated, aimed at stealing sensitive information, or disrupting computer systems, among other purposes.

Doctrine of Mens Rea and Actus Reus in Cyberbullying

In criminal law, the concepts of mens rea (the guilty mind) and actus reus (the guilty act) are crucial for establishing liability. These principles are equally applicable in cases of cyberbullying, a form of harassment that uses electronic means to intimidate, threaten, or humiliate others. Actus reus in cyberbullying involves the specific actions taken by the perpetrator, such as sending threatening emails, posting harmful content on social media, or disseminating private information without consent. On the other hand, mens rea relates to the perpetrator's intent to cause harm or reckless disregard for the impact of their actions.

The paper titled "Cyberbullying–A Critical Analysis of Laws, Criminal Responsibility and Jurisdiction" by Nibras Salim Khudhair, published in 2021[3], provides an insightful examination of the legal landscape concerning cyberbullying, with a focus on the application of traditional legal principles such as actus reus (the guilty act) and mens rea (the guilty mind)

[2] Mittal, Sandeep and Sharma, Priyanka, A Review of International Legal Framework to Combat Cybercrime (June 20, 2017). International Journal of Advanced Research in Computer Science, ISSN No. 0976-5697, Volume 8, No. 5, May-June 2017, Available at SSRN: https://ssrn.com/abstract=2978744 or http://dx.doi.org/10.2139/ssrn.2978744 (Last visited 14, May,2024)

[3] Salim, Nibras. *"Cyberbullying - A Critical Analysis of Laws, Criminal Responsibility and Jurisdiction." Journal of Contemporary Issues in Business and Government* 27 (2021): https://doi.org/10.47750/cibg.2021.27.03.317 (last visited March 2, 2024).

in the realm of digital interactions. This analysis is particularly relevant in common law jurisdictions, where these concepts form the cornerstone of criminal liability. The author discusses the difficulty in applying the actus reus requirement to cyberbullying, as the harmful act may not involve physical contact or may occur across different jurisdictions. Similarly, establishing mens rea involves determining the intent behind online actions, which can be obscured by anonymity and the digital nature of communication.

To prosecute a cyberbullying case effectively, it is necessary to prove that the accused not only committed the act of bullying but also possessed the requisite mental state to intimidate, harass, or harm the victim. This intersection of mens rea and actus reus in cyberbullying highlights the complexity of addressing such conduct legally, underlining the need for clear evidence of both the harmful action and the intent behind it.

History of Cyberbullying

Cyberbullying, a form of harassment that occurs through electronic means, has become a significant concern in the digital age. The history of cyberbullying is closely tied to the evolution of technology and the internet, with its roots tracing back to the early days of online communication.

In the 1990s, as the internet became more accessible to the general public, online forums, chat rooms, and email provided new platforms for interaction. These early forms of digital communication also became the first venues for cyberbullying. Users could hide behind the anonymity of the internet to send harassing or threatening messages without fear of immediate repercussions.

The term "cyberbullying" itself began to gain recognition in the early 2000s as researchers and educators started to notice the growing trend of online harassment, especially among school-aged children and teenagers. The rise of social media platforms such as MySpace, Facebook, and Twitter in the mid-2000s further exacerbated the issue. These platforms allowed bullies to reach a wider audience and provided new tools for harassment, such as public shaming, exclusion, and the spreading of rumors.

One of the first widely publicized cases of cyberbullying was the tragic story of Megan Meier[4], a teenager who took her own life in 2006 after being harassed on MySpace. This case brought national attention to the issue and sparked debates about the role of social media

[4] Moreno, G. "Cases of Victimization: Case 1: Megan Meier (Missouri, 2006)." *Preventing School Failure: Alternative Education for Children and Youth 55,* no. 2 (2011): 70. https://doi.org/10.1080/1045988X.2011.539465 (last visited March 2, 2024).

companies in preventing cyberbullying. In response to growing concerns, laws and policies began to evolve. The U.S. federal government addressed cyberbullying in the Higher Education Opportunity Act of 2008, and many states enacted their own legislation to protect victims and penalize perpetrators. Schools also started to implement anti-bullying policies that included measures to combat cyberbullying.

The advent of smartphones and mobile internet further changed the landscape of cyberbullying. With constant access to social media and messaging apps, victims could be harassed at any time and place. Cyberbullying became a 24/7 phenomenon, making it even more challenging to escape the harassment. The late 2000s and early 2010s were marked by a growing awareness of cyberbullying, prompting legal and societal responses. The Information Technology Act of 2000, amended in 2008, included provisions to address cybercrimes, although specific laws against cyberbullying were still lacking. Schools and educational institutions began incorporating cyber etiquette and safety into their curriculums, emphasizing the importance of responsible online behavior.

During the late 2010s and early 2020s have been characterized by a more proactive approach to combat cyberbullying. The government launched initiatives such as the Cyber Crime Prevention against Women and Children (CCPWC)[5]portal for reporting cybercrimes . Non-governmental organizations and activists have been instrumental in raising awareness and providing support to victims. Despite these efforts, cyberbullying remains a pervasive issue in India, with the COVID-19 pandemic further amplifying the problem due to increased online activity[6]. The anonymity of the internet, combined with societal issues such as gender discrimination and lack of digital literacy, continues to fuel cyberbullying.

As awareness of cyberbullying grew, so did efforts to combat it. Non-profit organizations, such as the Cyberbullying Research Center, were established to provide resources and support for victims and to conduct research on the issue. Educational campaigns aimed at teaching young people about digital citizenship and the importance of respectful online behavior became more common.

In recent years, artificial intelligence and machine learning technologies have been employed to detect and prevent cyberbullying. Social media companies have started using algorithms to identify and remove harmful content, and schools have adopted monitoring

[5] National Cyber Crime Reporting Portal, Ministry of Home Affairs, https://cybercrime.gov.in (last visited 2 Mar.2024)

[6] Ojasvi Jain, Manoj Gupta, Shreeya Satam & S.P. Panda, *Has the COVID-19 Pandemic Affected the Susceptibility to Cyberbullying in India?,* 2 Computers in Hum. Behav. Rep. 100029, 100029 (2020), https://www.sciencedirect.com/science/article/pii/S2451958820300441 (last visited 3 May.2024).

software to protect students. Despite these efforts, cyberbullying remains a pervasive problem. The anonymity of the internet, the ease of spreading information, and the increasing amount of time people spend online all contribute to the challenge of eradicating cyberbullying. As technology continues to evolve, so too will the methods of cyberbullying, requiring ongoing vigilance and adaptation in our strategies to combat it.

Theories Related to Cyberbullying Against Women

Several theoretical frameworks can help to understand the complex phenomenon of cyberbullying against women. These theories examine the psychological, sociological, and cultural contexts that contribute to the perpetuation of cyberbullying in digital spaces.

1.Social Learning Theory

Social Learning Theory, developed by Albert Bandura, posits that people learn from one another via observation, imitation, and modeling. In the context of cyberbullying, this theory suggests that individuals may adopt aggressive behaviors if they observe such actions being rewarded or not punished in their environment, whether offline or online. This theory is particularly relevant in explaining how societal norms and behaviors are replicated on social media, potentially leading to cyberbullying.[7] The theory emphasizes the role of peer influence and media exposure in shaping aggressive behaviors online.

2.Feminist Theory

Feminist theory provides a critical framework for understanding cyberbullying against women, focusing on the power dynamics and gender inequalities that pervade both real and virtual spaces. It argues that cyberbullying is a reflection of broader societal misogyny and sexism, where women are targeted in online environments due to their gender. This theory underscores the need to address underlying social structures and attitudes towards women to effectively combat cyberbullying.

3.Routine Activity Theory

Originally used to analyze patterns of crime and victimization, Routine Activity Theory can be adapted to the digital age, positing that cyberbullying occurs when there is a motivated offender, a suitable target, and the absence of a capable guardian. In the context of cyberbullying against women, the "suitable target" often includes accessible and visible profiles on social media, while the lack of capable guardians refers to the inadequate

[7] Ching Lei Li, Thomas Holt, Adam Bossler & David May, Examining the Mediating Effects of Social Learning on the Low Self-Control–Cyberbullying Relationship in a Youth Sample, 37 Deviant Behav. 126, 126-138 (2016), https://doi.org/10.1080/01639625.2014.1004023 (last visited Apr. 15, 2024).

monitoring and regulation of online behavior. For instance, the more women engage in online activities without sufficient digital guardianship, the more they are exposed to potential cyber threats[8]

4.Power-Control Theory

This theory, which emerges from criminology, explores the relationship between familial control dynamics and the propensity for delinquency, including cyberbullying. Power-Control Theory suggests that in households where traditional gender roles are strongly enforced, females might be both less likely to engage in and more likely to be victims of cyberbullying, reflecting broader societal norms about gender and control. In the context of gender, this often translates into men exerting control over women through cyber threats and harassment.[9]

5.Technology Acceptance Model (TAM)

Though primarily focused on the adoption of technology, the Technology Acceptance Model can also be useful in understanding how the ease of use and perceived usefulness of digital platforms contribute to cyberbullying. For example, if technology is easy to use for malicious purposes and perceived as an effective way to exert control or inflict harm, it may facilitate cyberbullying behaviors. This model assesses how perceptions of ease of use and usefulness impact the adoption of technology, potentially affecting exposure to online risks[10]

These theories collectively highlight that cyberbullying against women is not just an issue of individual behavior but is deeply embedded in cultural, social, and technological contexts. Addressing it requires a comprehensive approach that considers these multifaceted influences.

Distinction Between Cyberbullying and Traditional Bullying

Cyberbullying and traditional bullying against women are distinct phenomena, though both share the fundamental intent of harming or intimidating the target. Traditional bullying involves direct, face-to-face interactions that can include verbal insults, physical aggression, or social exclusion, typically occurring in settings like workplaces, schools, or community spaces. This form of bullying is limited by physical proximity and often leaves behind tangible evidence of the abuse.[11]

---

[8] Michael Arntfield, Towards a Cybervictimology: Cyberbullying, Routine Activities Theory, and the Anti-Sociality of Social Media, 40 Can. J. Comm. (2015), https://doi.org/10.22230/CJC.2015V40N3A2863 (last visited Apr. 15, 2024).

[9] Raymond Wong, Cheukfan Cheung & Baohua Xiao, Does Gender Matter in Cyberbullying Perpetration? An Empirical Investigation, 79 Comput. Hum. Behav. 247, 247-257 (2018), https://doi.org/10.1016/j.chb.2017.10.022 (last visited Apr. 25, 2024).

[10] Neil Brody & Anita Vangelisti, Cyberbullying: Topics, Strategies, and Sex Differences, 75 Comput. Hum. Behav. 739, 739-748 (2017), https://doi.org/10.1016/j.chb.2017.06.020 (last visited Apr. 25, 2024).

[11] Meyran Boniel-Nissim, Cyberbullying vs. Traditional Bullying – Do Victims React Differently? in Psychological Applications and Trends 2019, https://doi.org/10.36315/2019inpact101 (last visited Apr. 25, 2024).

Cyberbullying, on the other hand, occurs in the digital realm. It includes sending threatening emails, posting derogatory comments on social media, or disseminating private information without consent. A key distinction is that cyberbullying allows the perpetrator to hide behind the anonymity of the internet, potentially reaching a vast audience. This anonymity can embolden bullies, as the perceived lack of direct consequences can lead to more extreme behavior compared to traditional bullying. Additionally, the effects of cyberbullying can be more pervasive and persistent, as digital content can be difficult to remove and may continue to affect the victim indefinitely.

In the context of impacts on women, both types of bullying can exacerbate existing gender inequalities and have severe emotional and psychological consequences. However, cyberbullying uniquely allows for continuous harassment that can follow victims across various platforms, infringing on their sense of safety and well-being in what might otherwise be private spaces.

Forms and Manifestations of Cyberbullying Against Women

Cyberbullying against women manifests in various forms, each exploiting digital platforms to harass, intimidate, or demean. Understanding these forms is crucial for recognizing and addressing the specific challenges women face online.

Harassment: This involves sending aggressive or obscene messages through social media, emails, or messaging apps. Harassment can be persistent, with bullies sending repeated unsolicited messages that can include threats, insults, or unwanted sexual advances. This form of cyberbullying is particularly invasive as it disrupts the victim's personal space and can lead to severe anxiety and distress. The Ritu Kohli case[12] is often cited as one of the first well-documented instances of cyberstalking in India, which brought attention to the need for specific laws addressing cyber harassment. This case occurred in the late 1990s, when the internet was still relatively new in India. It was the first reported cyber sex crime in India.

It was reported on Sunday, June 18, 2000 in Delhi. In this case a 30-year-old software engineer, Manish Kathuria, was arrested by officials of the Crime Branch of the Delhi police for harassing a woman by chatting on the internet. Manish reportedly used to chat on website www.micr.com under the name of Mrs. Ritu Kohli. He used obscene languages while chatting and also gave her residential telephone number for further chatting. As a result, Mrs. Kohli started getting obscene calls at her residence. Due to the disturbances, Mrs. Kohli lodged a

[12] Vishi Aggarwal & Ms. Shruti , Cybercrime Victims: A Comprehensive Study , 6 , IJCRT, 646, 2018.(Last visited 15, may.2024)

complaint and after the enquiries the Delhi police traced the culprit and started criminal proceedings against him under section 67 of IT Act with section 509 of IPC for outraging Ritu Kohli‟s modesty.

Doxing: This form of cyberbullying involves researching and broadcasting private or identifying information about an individual without their consent. For women, doxing can include the publication of personal addresses, phone numbers, or even financial information, exposing them to greater risks of stalking and physical harm. For example in the case of Climate activist Disha Ravi[13] was arrested in connection with a toolkit related to the farmer protests, which had been tweeted by Greta Thunberg. After her arrest, her personal details, including her home address and contact information, were circulated on social media, leading to severe online harassment[14].

Cyberstalking: Similar to traditional stalking but conducted online, this involves the persistent monitoring, harassing, or threatening of an individual via digital channels. Cyberstalking can include keeping tabs on the victim's online activities, sending threatening messages, and manipulating the victim by online information. In the case of Rajnesh Kumar v. State of Himachal Pradesh (2018)[15], the Himachal Pradesh High Court affirmed that Section 354D of the IPC could be invoked in cases of cyberstalking, emphasizing the need to protect individuals from harassment and intimidation in the digital realm. Karan girotra v. State & anr:- This case was reported on 8th May 2012 on cyber stalking when the petitioner filed an application to grant anticipatory bail. This case dealt with a woman, Shivani Saxena, whose marriage could not be consummated, and she filed a divorce with mutual consent. In between, she came across Karan Girotra while chatting on the internet, who told her that he loved her and wanted to marry her. Girotra invited Saxena over to his house to introduce her to his family where he intoxicated her and sexually assaulted her. He started assuring her that he would marry her and began sending her obscene pictures of her assault. He also threatened her to circulate the pictures if she would not marry him. As a result, an engagement ceremony was performed after which he continued to assault her and called off his engagement to her. Frustrated out of this, Saxena filed a complaint under section 66-A of the IT Act. Although the court rejected the plea of anticipatory bail but did not give serious custodial interrogation.[16]

[13] Disha A. Ravi v. State (Nct Of Delhi) & Ors., AIRONLINE 2021 DEL 159

[14] Deccan Herald, Toolkit Case: Did Not Leak Disha Ravi's Private Chats to Media, Delhi Police Tells HC (Aug. 5, 2021, 12:33 PM), https://www.deccanherald.com/india/toolkit-case-did-not-leak-disha-ravis-private-chats-to-media-delhi-police-tells-hc-1016555.html.

[15] Rajneesh Kumar Sharma vs State Of Himachal Pradesh And Others on 8 October 2018

[16] AravinthBalakrishnan:Challenges In Regulating Cyberstalking At The Cyber Space, www.legalserviceindia. Com (last visited May.15,2024)

Revenge Porn: This particularly malicious form targets individuals by sharing intimate, private media without consent. Often used as a form of control or retaliation, revenge porn can devastate a person's reputation, personal relationships, and career, leading to long-term psychological trauma. India's first-ever case of revenge porn was that of State of West Bengal v. Animesh Boxi, a 2018 case. The accused, Animesh Boxi (alias Animesh Bokshi alias Animesh Bakshi) was in a relationship with the victim (her name was not disclosed to protect her identity) for three years prior to the incident that occurred in July 2017. Over the course of the relationship, Boxi demanded intimate photos from the victim and allegedly "hacked into her phone" to get his hands on them. He then started blackmailing her, saying that he would upload the photos and videos online if she refused to spend time with or "go for outings with" him . A few days later, the victim's brother discovered the nude pictures and videos on a porn site (PornHub) with the video which gave the victim's name and also identified her father[17]. Boxi was charged under sections 354A (Sexual Harassment), 354C (Voyeurism), 354D (Stalking) and 509 (Criminal Intimidation) of the Indian Penal Code, 1860 ("IPC") and sections 66C (Identity theft), 66E (Violation of privacy) and 67/67A (Transmitting obscene material online) of the Information Technology Act 2000 ("IT Act").

Trolling[18]: This involves posting inflammatory, derogatory, or provocative messages aimed at provoking or upsetting individuals. Women are often targeted in gender-specific ways, including sexist attacks or comments that can be particularly demeaning and emotionally damaging. Recently in March 2024, a women named Geethanjali committed suicide due to online trolling. The language used by some of the trolls is highly objectionable and she felt humiliated and insulted and it drove her to take the extreme step.[19]

Identity Theft and Impersonation: Perpetrators may steal a woman's identity to embarrass or discredit her, or to commit fraud. Impersonating someone online can also involve creating fake accounts to post inappropriate or harmful content in their name.

Body Shaming and Image-Based Abuse: This can involve posting derogatory comments about a woman's appearance or sharing manipulated photos of her without consent. Such

---

[17] State of West Bengal v. Boxi, Global Freedom of Expression, https://globalfreedomofexpression.columbia.edu/cases/state-of-west-bengal-v-boxi/, last visited Apr. 27, 2024.

[18] "8 of 10 Urban Indian Women Now Using Internet but Harassment, Trolling Key Concerns: LocalCircles Survey," The Economic Times, https://economictimes.indiatimes.com/news/india/8-of-10-urban-indian-women-now-using-internet-but-harassment-trolling-key-concerns-localcirclessurvey/articleshow/98455226.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst (last visited Apr. 27, 2024).

[19] "Police Arrest Two in Connection with Geethanjali Social Media Trolling Case," The Hindu, https://www.thehindu.com/news/national/andhra-pradesh/police-arrest-two-in-connection-with-geethanjali-social-media-trolling-case/article67951340.ece (last visited Apr. 27, 2024).

actions are aimed at shaming the victim and can lead to significant emotional distress. In the Sakshi Malik Case (2021)[20] Model and actress filed a lawsuit against the makers of the film "Venom" for using her image without permission in a derogatory manner, which led to body shaming and character assassination on social media. The Bombay High Court ordered the removal of the scenes with her image, underscoring the importance of consent and the impact of misuse of images leading to body shaming.

Each of these forms of cyberbullying leverages the anonymity and reach of the internet, allowing bullies to operate covertly and often without immediate consequence. The impact on women can be profoundly damaging, affecting their mental health, social relationships, and overall well-being. It's crucial for digital platforms to enforce strong anti-bullying policies and for legal frameworks to catch up to protect individuals from these increasingly common forms of abuse.

Why Women Are More Prone to Cyberbullying Than Men in India

Women being more prone to cyberbullying than men in India is a multifaceted issue rooted in societal, cultural, and technological dynamics. There are several key factors that contribute to this phenomenon such as:

1.Gender Norms and Social Expectations:

In many parts of India, traditional gender roles are strongly enforced, and women are often expected to adhere to conservative norms concerning behavior and self-expression. When women challenge these expectations by being vocal or visible online, they may become targets of cyberbullying intended to enforce conformity or punish non-conformity. A notable example that illustrates the impact of gender norms and social expectations on women experiencing cyberbullying in India is the case of Rana Ayyub[21], a prominent Indian journalist. This case study underscores the challenges women face when they are vocal and visible in digital spaces, particularly when their work challenges entrenched societal and political norms. Rana Ayyub has been subjected to extensive cyberbullying, including death threats, rape threats, and severe online harassment. Her social media accounts, particularly Twitter, have been inundated with abusive comments and hate speech. The case has drawn international condemnation from global watchdogs and human rights organizations, which have called on Indian authorities and

[20] Sakshi Malik vs Venkateshwara Creations Pvt Ltd on 2 March 2021,IP Suit No.3510 of 2021

[21]RanaAyyub:Availableat:https://www.icfj.org/sites/default/files/202302/Rana%20Ayyub_Case%20Study_ICFJ.pdf (Last visited 29 April 2024).

global platforms to provide better protection for women like Ayyub.[22]

2. Digital Literacy and Access:

While internet usage is rising rapidly among women in India, there remains a gender gap in digital literacy. Lower levels of digital literacy can make women more vulnerable to online harassment, scams, and bullying because they may be less aware of privacy settings, the implications of sharing information online, and ways to report or address harassment. A case study that illustrates this issue involves a project conducted by the Digital Empowerment Foundation (DEF) in several rural areas across India. The main goal of DEF's initiative was to increase digital literacy among rural women to help them become more adept at using technology safely and effectively. This included understanding how to utilize the internet, manage digital accounts, and safeguard personal information online. DEF conducted workshops and training sessions in villages across states like Rajasthan, Madhya Pradesh, and Bihar.

3. Sexual Harassment:

Women online are often subjected to sexual harassment, which is a prevalent form of cyberbullying. This can include unsolicited sexual advances, revenge porn, stalking, and the sharing of manipulated images. Such actions are often used to intimidate and silence women. A notable case that highlights these issues is the incident involving a group called "Bois Locker Room"[23]in India. In May 2020, an Instagram scandal, widely known as the "Bois Locker Room," was uncovered involving a group of teenage boys from prominent schools in Delhi, India. The boys used this private Instagram group to share obscene and morphed images of underage girls, objectifying them and discussing acts of sexual violence against them.

4. Anonymity of the Internet:

The anonymous nature of the internet can embolden perpetrators, as they feel they can avoid the consequences of their actions. This anonymity can lead to an increase in gender-based harassment as aggressors feel shielded from repercussions. One notable case that highlights the role of internet anonymity in exacerbating gender-based harassment involves the Indian actress Rhea Chakraborty. Her case illustrates how the anonymity of the internet can

[22] UN experts call on India to protect journalist Rana Ayyub from online hate campaign | ohchr. Available at: https://www.ohchr.org/en/press-releases/2018/05/un-experts-call-india-protect-journalist-rana-ayyub-online-hate-campaign (Last visited 29 April 2024).

[23] Archana Sharma vs State Of Nct Of Delhi & Ors on 20 May, 2020

fuel harassment and exacerbate the challenges faced by women in the public eye.[24]

5. Cultural Stigma and Victim-Blaming:

Women who experience cyberbullying often face additional societal stigma. The blame is frequently placed on the victim, with questions raised about their online activity, the time they spend online, and the nature of their interactions. This societal stigma can have devastating effects on women's well-being and mental health. It can make them feel ashamed, isolated, and reluctant to seek support. Additionally, the fear of being blamed or judged may prevent them from speaking out about their experiences, perpetuating a cycle of silence and suffering.

In conclusion, women in India are disproportionately affected by cyberbullying due to a combination of social, cultural, and systemic factors. Deep-rooted gender inequalities, cultural attitudes toward women, and the normalization of violence contribute to a climate where online harassment against women is prevalent and often goes unaddressed. Additionally, intersecting forms of discrimination based on factors such as caste, religion, sexuality, and socioeconomic status further exacerbate women's vulnerability to cyberbullying. Only through concerted efforts to address these root causes can we create a safer and more inclusive online environment for women in India.

Psychological Impact of Cyberbullying

Cyberbullying has a significant psychological impact on its victims, particularly women, who often experience intense emotional and psychological distress. When women are targeted in cyberbullying incidents, the effects can be deeply traumatic, leading to a wide range of psychological outcomes.

One of the most immediate and prominent impacts is the development of anxiety and depression. Victims may experience persistent worry, sadness, and a sense of helplessness, which can escalate into clinical anxiety or depressive disorders. The anonymity and pervasiveness of online platforms can make the harassment feel inescapable, exacerbating these feelings. Women may also suffer from a diminished sense of self-worth and self-esteem, leading to deeper emotional turmoil and withdrawal from social interactions.

Furthermore, the fear of public humiliation and stigmatization can lead to social anxiety, where victims feel intensely afraid of further interactions, not just online but also in physical settings. This can disrupt personal relationships and hinder professional or educational

[24] TARGETED HARASSMENT: THE MEDIA-LED WITCH HUNT OF RHEA CHAKRABORTY By Poornima Rajeshwar(https://mediamanipulation.org/case-studies/targeted-harassment-media-led-witch-hunt-rhea-chakraborty) (last visited 15 may,2024)

opportunities, as the victim might avoid situations where they feel vulnerable to public scrutiny or further attacks.

In more severe cases, the relentless nature of cyberbullying can lead to post-traumatic stress disorder (PTSD), where the victim relives their experiences through flashbacks and nightmares, remaining in a state of heightened alertness and emotional distress. Additionally, there is an increased risk of suicidal thoughts and behaviors among victims of cyberbullying, especially if the harassment is prolonged and support systems are lacking.

The cumulative effect of these psychological impacts necessitates robust support systems, including counseling and legal recourse, to help victims cope and recover. It's also vital for society to foster safe online environments and educate individuals about the harms of cyberbullying and the importance of digital etiquette and empathy.

Legal Framework

1.The Information Technology Act:

The Information Technology (IT) Act of 2000 was established in India and took effect on October 17, 2000. This legislation applies across India but also has extraterritorial reach, meaning it applies to offenses committed outside of India by any person, irrespective of their nationality, if the offense involves a computer, computer system, or computer network located within India. This is articulated through the combination of Section 1(2) and Section 75 of the IT Act.

The primary aim of the IT Act is to provide a legal framework for electronic transactions executed via electronic data interchange and other forms of electronic communication, which are collectively referred to as "electronic commerce." These digital methods are intended to serve as substitutes for traditional paper-based techniques in communication and information storage. Additionally, the Act is designed to facilitate the electronic filing of documents with government entities and amends several significant legal statutes, including the Indian Penal Code (1860), the Indian Evidence Act (1872), the Bankers' Books Evidence Act (1891), and the Reserve Bank of India Act (1934). The IT Act of 2000 is inspired by the Model Law on Electronic Commerce, which was adopted by the United Nations Commission on International Trade Law (UNCITRAL) in 1996.

Chapter XI of the Information Technology Act of 2000[25] addresses cyber offenses, where both the action (actus reus) and the intention (mens rea) to commit the act are present. This law

[25] Information Technology Act, No. 21 of 2000 (India)

specifically pertains to offenses involving the use of information technology either as a means to perpetrate the crime or as the focus of the crime itself. Although there are no specific laws to regulate cyberbullying in India, we do have **Section 66A**[26] of the Information Technology Act. This Act prescribes the punishment for sending annoying, offensive, and insulting communication through digital and information communication technology.

Before it was declared unconstitutional in the Shreya Singhal case[27], Section 66A of the Information Technology Act outlined penalties for transmitting information deemed grossly offensive or menacing via a computer resource or communication device. Additionally, it prescribed punishment for disseminating knowingly false information with the intent to cause annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will repeatedly. Moreover, sending electronic messages to cause inconvenience, annoyance, or to mislead the recipient about the sender's identity was also punishable by imprisonment for up to three years and a fine.

Section 66C[28] addresses the offense of identity theft, stipulating that individuals who fraudulently or dishonestly utilize another person's electronic signature, passwords, or other distinct identification features can face imprisonment for up to three years and a fine of up to Rs. 1 Lakh. The primary distinction between "identity theft" and "cheating by personation" lies in the fact that the former involves the actual theft of someone's identity, whereas the latter may involve impersonation of either a real individual or a fictional one. Furthermore, identity theft specifically requires the use of a unique identifier, while personation can be accomplished through various means.

Section 66E[29] of the law is designed to safeguard individuals' privacy, particularly concerning the intentional or knowingly capturing, publishing, or distribution of images, whether in printed or electronic form, depicting a person's private areas without their consent. This provision addresses violations of bodily privacy, such as those occurring in instances like MMS clips. Offenders can face imprisonment for up to three years, a fine not exceeding 2 lakh rupees, or both. It's crucial to note that Section 66E covers each stage of violating bodily privacy capturing, publication, and transmission of images when done without the victim's consent.

Section 67 of the IT Act, 2000 delineates penalties for electronically publishing or

[26] Section 66A has been struck down by Supreme Court's Order dated 24th March, 2015 in the Shreya Singhal vs. Union of India, AIR 2015 SC. 1523
[27] ibid 47
[28] Information Technology Act, No. 21 of 2000, §.66C
[29] Information Technology Act, No. 21 of 2000, § 66E

transmitting obscene material. Such actions can result in imprisonment for up to three years and a fine of up to 5 lakh rupees. For subsequent convictions, the penalties increase, with imprisonment extending up to five years and a fine of up to 10 lakh rupees.

This section holds significant historical importance as it marked the first-ever conviction under the IT Act 2000 in India. The case "State of Tamil Nadu vs Suhas Katti"[30] on 5 November 2004 demonstrated the efficacy of this section and the reliability of electronic evidence. The prosecution successfully proved the strength of the section by securing a conviction in a case involving cyber stalking, email spoofing, and the offenses outlined in this section, including sending obscene messages in the name of a married woman.

Section 67 of the IT Act, 2000 outlines penalties for electronically distributing or transmitting obscene materials. Additionally, the IT (Amendment) Act of 2008 introduced two more sections: **Section 67A**, which addresses punishment for electronically disseminating sexually explicit acts, **and Section 67B**, which prohibits the distribution of child pornography.

2.The Indian Penal Code,1860

Cyberbullying, a form of harassment or bullying that occurs through electronic means, has become increasingly prevalent with the rise of digital communication. In India, while the term "cyberbullying" itself is not explicitly mentioned in the Indian Penal Code (IPC), various sections of the IPC and other relevant legislations address actions that constitute cyberbullying, especially when directed towards women. These legal provisions are crucial in safeguarding the dignity, privacy, and security of women in the digital space.

Section 292 A of the Indian Penal Code, 1860[31] -This section addresses the issue of producing any material in a grossly indecent way or with the intention of blackmail. It covers the activities of printing, selling, or distributing any printed or written document that is deemed indecent or meant for blackmail. It also criminalizes participating in or profiting from the business involving the sale, import, export, or printing of such materials, or advertising them, as these acts are considered harmful to morality. Offenders are subject to legal penalties under this section.

Section 354 C of the Indian Penal Code, 1860[32]- This section pertains to voyeurism. It specifies that if a man captures or views images of a woman engaged in a private act under circumstances where she expects privacy, or if he disseminates such images to others, it constitutes an offense. This law is specifically applicable to males; females are not subject to

[30] State of Tamil Nadu v. Suhas Katti, CC No 4680/2004 order dated November 5, 2004
[31] Indian Penal Code § 292A
[32] Indian Penal Code § 354C

punishment under this statute. The punishment for a first-time offender includes imprisonment ranging from one to three years and a fine, with subsequent offenses resulting in increased imprisonment of three to seven years along with a fine.

Section 354 D of the Indian Penal Code, 1860[33]- This section defines the crime of stalking as follows: it occurs when a man follows or contacts a woman, or attempts to engage her in personal interaction frequently despite her clear lack of interest. It also includes monitoring a woman's online activities through various communication methods such as email or messaging apps. This section exclusively addresses the stalking of women; stalking of men is not covered. In the State of West Bengal v. Animesh Boxi (2018), the accused was found guilty under this section after hacking a woman's phone, obtaining private photos, and threatening to distribute them on an adult site, an act the court equated to virtual rape.

Section 499 of the Indian Penal Code, 1860[34] - This section is concerned with defamation, which is broadly defined to include both traditional forms (written or oral) and online expressions that are posted on digital platforms and potentially damage someone's reputation. Those found guilty of online defamation can be punished under Section 500, which includes penalties of up to two years in prison, a fine, or both.

Section 507 of the Indian Penal Code, 1860[35] - This section deals with criminal intimidation executed through anonymous communications. It targets individuals who use a false identity or an unknown telecommunication source, such as social media, to threaten others. The prescribed punishment can include up to two years of imprisonment.

Section 509 of the Indian Penal Code, 1860[36]- This section addresses acts, words, gestures, or sounds intended to invade a woman's privacy or offend her modesty. The law emphasizes the offender's intent as a critical element. Penalties for harassing a woman through electronic means or telecommunication devices include a minimum of two months to two years of rigorous imprisonment and a possible fine.

3.The Indecent Representation of Women (Prohibition) Amendment Bill, 2012[37]

The Bill, introduced in the Rajya Sabha on December 13, 2012, aims to modify the Indecent Representation of Women (Prohibition) Act, 1986. Originally, this Act focused primarily on preventing the indecent depiction of women in advertisements or through

[33] Indian Penal Code § 354D
[34] Indian Penal Code § 499
[35] Indian Penal Code § 507
[36] Indian Penal Code § 509
[37] TheIndecentRepresentationofwomen(prohibition)Availableat: https://prsindia.org/files/bills_acts/bills_parliament/2012/SCR-Indecent_Representation_of_Women.pdf.

publications, writings, and paintings, which were largely confined to print media. The proposed amendments in the Bill intend to expand the Act's reach to encompass newer forms of communication. It seeks to prohibit the publication or distribution of any content featuring indecent representation of women across various media. Additionally, the Bill broadens the definition of "advertisement" to include both printed and electronic forms, extending to digital platforms, electronic messages (SMS, MMS), and outdoor advertising such as hoardings. The Committee has recommended that this definition should be further extended to cover all forms of advertising through any medium. The Indecent Representation of Women (Prevention) Act and the proposed amendments to it can fill in the long-needed legal requirements for preventing cyber victimisation of women in India. But the provision and the proposed amendments are not flawless. The proposed amendments basically highlight two issues - extending the scope of the law to digital mechanism to victimise women and bringing in the penalties to be at par with the penalties as prescribed in the Information Technology Act, especially under sections 67 and 67 A. It is definitely a welcome move however the bill was withdrawn from Rajya Sabha in 26th July 2021.[38]

4.The Protection of Children From Sexual Offences Act, 2012

The Protection of Children from Sexual Offences Act (POCSO Act), enacted in 2012, is specifically designed to protect children (individuals under the age of 18) from sexual abuse and exploitation, including through digital means. While the POCSO Act primarily focuses on children, its relevance to cyberbullying against women arises in scenarios where the victims are underage females. The Act criminalizes the use of a child in any form of media (including electronic and online) for sexual purposes, which includes the production, distribution, and consumption of child pornography. This extends to cyberbullying when the harassment includes the sharing or creation of explicit images of underage girls. There is No specific mention of online sexual harassment in Indian law, but sections can be interpreted to cover it as they use words such as "electronic" and "digital". Section 11,12 of the POCSO Act, 2012: sexual harassment of a child, cognizable and bailable offense, punishment of imprisonment up to 3 years and fine. Their related crimes are cyberstalking, cyberbullying, child pornography etc,.

https://prsindia.org/billtrack/the-indecent-representation-of-women-prohibition-amendment-bill-2012 (Last visited 2 may 2024)

Government Initiatives

1. The Nirbhaya Fund Scheme: Launched by the Government of India, the Nirbhaya Fund is dedicated to enhancing the safety of women and children. As part of this initiative, the Ministry of Home Affairs introduced a unified emergency number (112) managed by the Emergency Response Support System (ERSS). This number facilitates immediate access to police, fire services, rescue operations, and other urgent assistance.
2. Cyber Crime Prevention Against Women and Children (CCPWC)[39]: This program sets up various divisions responsible for the reporting and investigation of online crimes, processing cybercrime complaints, and identifying serious cybercrime issues. The total funding for this scheme is approximately Rs. 223.198 crores, and it includes several components:
    - An online platform for reporting cybercrimes
    - A national cyber forensic laboratory
    - Training programs for police officers, judges, and prosecutors
    - Cybercrime awareness initiatives
    - Research and development efforts
3. Indian Cybercrime Coordination Centre (I4C) Scheme[40]: The I4C acts as a comprehensive tool against cybercrime in India, managing cybercrime prevention efforts in a coordinated manner and reducing the misuse of online spaces. Supported by international organizations and technological advancements, I4C focuses on the issues posed by internet media, particularly protecting women and children. It also promotes rapid reporting of financial fraud to prevent monetary theft.
4. Cybercrime Reporting Portals and Helplines:

   National Cyber Crime Reporting Portal: This portal, a Government of India initiative, provides a platform for victims, especially women and children, to file online complaints about cybercrimes. It offers quick response to complaints with local police support, surpassing traditional methods in speed and efficiency. The portal enables nationwide complaint registration, facilitating easy access to cybercrime cells and essential information. Victims can also contact local cyber crime cells as an alternative to online reporting.

[39] National Commission for Women. Available at: http://ncw.nic.in/ncw-cells/legal-cell/new-bills-laws-proposed/cyber-crime-prevention-against-women-and-children-ccpwc#:~:text=CYBER%20CRIME%20PREVENTION%20AGAINST%20WOMEN,CCPWC)%20%7C%20National%20Commission%20for%20Women (Accessed: 29 April 2024).

[40] (Indian Cybercrime Coordination Centre. Available at: https://i4c.mha.gov.in/ (last visited 29 April 2024).

State-wise Cyber Crime Portal: This portal lists contact details and email IDs of nodal cyber cell officers and grievance officers, available at https://cybercrime.gov.in/.

5. In response to a significant increase in bullying, particularly in boarding schools across India, the Ministry of Human Resource Development has established anti-ragging committees. These committees are tasked with disciplining students involved in bullying, which may include rustication for severe offenses. Additionally, the University Grants Commission (UGC) has implemented policies to curb ragging in higher education institutions, introducing specific anti-ragging measures for universities and colleges.
6. The Ministry of Home Affairs has launched a centralized online cybercrime reporting platform that allows victims to file complaints without needing to visit a police station. Furthermore, police departments in Delhi, Indore, and Uttarakhand have formed cyber squads that educate the public on how to file complaints online.

Role of Indian Judiciary

The Indian judiciary has become a formidable protector of digital liberties, especially amid increasing cybercrimes and online abuse. In recent years, courts have increasingly adopted proactive measures to interpret and broaden the law to recognize the distinct damages women encounter in the digital realm. The judiciary's function has evolved beyond the simple enforcement of established laws to the nuanced interpretation of constitutional concepts, like the right to privacy, dignity, and free speech, in the context of digital interactions. Occurrences of online abuse encompassing cyberstalking, revenge pornography, impersonation, and digital defamation have complicated the conventional interpretation of criminal responsibility, leading courts to establish more sophisticated frameworks. These court interventions have addressed legislative deficiencies and ensured accountability for perpetrators, even in instances where the law was previously silent or confusing.

The judiciary has acknowledged the psychological suffering and societal repercussions of online abuse, extending beyond traditional sentence to implement restitution, compensation, and institutional improvements. Judicial bodies have readily provided directives for the protection of victims, equating those subjected to digital harassment with survivors of sexual abuse for legal protections and reparations. They have analyzed the provisions of the Indian Penal Code and the Information Technology Act with discernment, emphasizing that online offenses are neither insignificant nor devoid of victims. Furthermore, by refusing bail in significant cybercrime instances and underscoring the necessity for enhanced regulatory

frameworks, the judiciary has conveyed a clear message regarding the imperative nature of digital security and accountability. The Indian judiciary is actively shaping a legal framework that addresses technological misuse with constitutional oversight and a robust commitment to justice. The below cases are the prime examples of role of judiciary in the cyberbullying.

Shreya Singhal v. Union of India (2015)[41]- This landmark Supreme Court case is crucial for understanding the legal landscape around online speech and harassment. The court struck down Section 66A of the Information Technology Act, 2000, which was often misused in cases of online harassment due to its broad and ambiguous wording. The judgment was significant in balancing the need for online speech protection while addressing abuse.

Kailash v. State of Maharashtra (2018) - This case involved instances of cyberbullying and stalking. The Bombay High Court emphasized the seriousness of cyberstalking and bullying, particularly when directed at women, and upheld stringent application of cyber laws to protect victims.

State of Tamil Nadu v. Suhas Katti (2004)[42] - One of the earliest cases involving cyber harassment, where the accused was successfully prosecuted for sending obscene and threatening messages to a woman. It was one of the first convictions under the Information Technology Act, 2000, setting a precedent for later cases.

State of West Bengal v. Animesh Boxi[43]- In 2018, the Tamluk session court in West Bengal delivered a pivotal ruling in the case of State of West Bengal v. Animesh Boxi, addressing the issue of revenge pornography. This case marked the first instance in which the accused was convicted and sentenced to five years of imprisonment, along with a fine of 9,000 rupees, for disseminating abusive and private images of the victim online without her consent. The relationship between the accused and the victim had been intimate, during which he acquired personal photographs and videos under the promise of marriage. After their separation, the accused uploaded these images and videos to pornographic websites using the names of the victim and her father. He was convicted under Sections 354, 354A, 354C, and 509 of the Indian Penal Code, as well as Sections 66E, 66C, 67, and 67A of the Information Technology Act. In a significant step, the court also directed the state government to treat victims of revenge pornography on par with rape survivors, ensuring they receive appropriate compensation, in addition to the penalties of fines and imprisonment already imposed.

[41] AIR 2015 SUPREME COURT 1523
[42] C No. 4680 of 2004
[43] State of West Bengal v. Animesh Boxi, C.R.M. No. 11806 of 2017, GR/1587/2017 (India)

State of Maharashtra v. Manish Kathuria[44]- In the discussion of cyberbullying and cyberstalking, the case of Ritu Kohli is significant. In 2001, Ritu Kohli reported that she was receiving persistent calls from various sources, including international ones, and that her identity had been used to upload deceptive content on social media. Manish Kathuria was identified as the offender who harassed Ms. Kohli using offensive language while stalking her on a chat service and subsequently leaking her contact details to numerous individuals.

Furthermore, Manish Kathuria impersonated Ms. Kohli and engaged in conversations on the website "www.mirc.com." Over the course of three days, Ms. Kohli endured approximately forty disparaging phone calls during the late hours. This harassment compelled her to file a complaint with the Delhi Police. The Delhi Police tracked down the IP addresses following her complaint and apprehended Mr. Kathuria. The Information Technology (IT) Act could not be applied as it had not been enacted when the complaint was lodged.

This incident marks the first documented case of cyberstalking in India. Although no further legal actions are recorded, this case prompted Indian legislators to recognize the need for laws addressing cyberstalking, leading to the amendment of the IT Act in 2008 to include Section 66-A, which penalized the sending of abusive messages via communication services. However, the validity of this section was challenged, and it was ultimately struck down by the Supreme Court in 2015, ruling that it infringed upon the right to free speech and expression.

State of Maharashtra v. Yogesh Prabhu[45]- In the 2009 case of State of Maharashtra v. Yogesh Prabhu, the accused and the victim, who were former acquaintances, engaged in an online conversation during which the accused proposed marriage. The victim declined, and the conversation ceased. Despite this, he continued to follow her online. The victim initially ignored emails containing obscene images and videos sent from an anonymous account, but eventually, she reported these incidents. The Cyber Crime Investigation Cell conducted an investigation, and the accused was convicted by a magistrate court under Section 509 of the Indian Penal Code (IPC), which deals with acts intended to insult the modesty of a woman, and Section 66E of the Information Technology Act, 2008, which addresses the violation of privacy. The enactment of Section 354D into the IPC, which specifically addresses stalking, was a direct outcome of this case.

In the case ***of Prakhar Sharma v. The State of Madhya Pradesh***[46], the accused created a fake Facebook account of the victim, posted some vulgar messages along with the photos of

[44] State of Maharashtra v. Manish Kathuria [2001](India)
[45] State of Maharashtra (cyber cell) v. Yogesh Pandurang Prabhu, C.C. NO. 3700686/PS/2009 (India)
[46] Prakhar Sharma v. The State of Madhya Pradesh, MCRC No. 377 of 2018.

the victim downloaded from her original Facebook account. The accused was charged under Sections 66 (c), 67 and 67(a) of the IT Act. When the accused applied for bail, it was denied by the Madhya Pradesh High Court.

***Shibani Barik v. State of Odisha*[47]-** In the case of Shibani Barik v. State of Odisha, Shibani Barik, along with co-accused Upendra Mahananda, was charged with both direct and indirect torture of the deceased, Late Padmalochan Barik, ultimately leading to his death. The co-accused, who had been romantically involved with Shibani Barik before and after her marriage to the deceased on February 21, 2019, sent private TikTok videos to the deceased that were also made public. These videos caused the deceased to experience feelings of betrayal and humiliation, contributing to his mental distress. Subsequently, he committed suicide by hanging himself from a ceiling fan in his bedroom. During the preliminary investigation, it became clear that the co-accused played a role in abetting the suicide. Shibani Barik was charged under Sections 306 and 34 of the Indian Penal Code, 1860. However, the evidence did not conclusively demonstrate her involvement in the crime, prompting the need for further evidence and documentation. Consequently, the court approved her bail application under Section 439 of the Criminal Procedure Code, citing the TikTok videos as a factor in the unfortunate loss of life and recognizing the increasing issue of harassment via inappropriate TikTok videos.

[47] Shibani Barik v. State of Odisha, AIRONLINE 2020 ORI 173

CHAPTER-III

ROLE OF SOCIAL MEDIA PLATFORMS- INTERMEDIARY REGULATION & CONTROL MEASURE

Social media platforms have become integral parts of modern communication, serving as avenues for connection, expression, and community-building. Their influence spans across diverse aspects of society, from personal relationships to political discourse and business marketing. With billions of users worldwide, social media platforms wield significant power in shaping public opinion and disseminating information. However, alongside their benefits, they also raise concerns about privacy, misinformation, and cyberbullying. Understanding the role of social media platforms entails examining their impact on individual behavior, societal dynamics, and global interactions.

Brief History and Evolution of Social Media Platforms

The evolution of social media platforms represents a dynamic chapter in the history of digital communication, beginning with the early internet days of the 1990s. The concept of social media started with sites like SixDegrees, which allowed users to create profiles and connect with others. By the early 2000s, platforms such as Friendster and MySpace gained popularity, introducing features that are now staples of social networking, such as customizable profiles and interactive friend networks.

The landscape of social media changed significantly with the launch of Facebook in 2004. Originally limited to college students, it eventually opened to the general public and quickly became the defining platform for social media worldwide. The evolution of significant platforms like Facebook reflects a shift from simple networking sites to complex infrastructures impacting various domains such as advertising and publishing. This transformation is characterized by constant updates in platform architecture, governance, and integration with other services [48].YouTube emerged in 2005, creating a new way for people to communicate and share through video. Twitter followed, launching in 2006 and offering a platform focused on brief, real-time posts that became immensely popular for its simplicity and immediacy.

The 2010s saw the rise of platforms like Instagram and Snapchat, which emphasized visual communication through photos and videos, appealing particularly to younger audiences.

[48] Helmond, A., Nieborg, D., & Vlist, F. (2019). Facebook's evolution: development of a platform-as-infrastructure.InternetHistories,3,12146.(Availableat:https://www.tandfonline.com/doi/full/10.1080/24701475.2019.1593667 (last visited 29 April 2024)

LinkedIn continued to evolve as a network for professional connections and career advancement, distinguishing itself from more personal and casual social platforms.

Recent years have seen the emergence of TikTok, which became rapidly popular with its short-form video content, and the expansion of messaging apps like WhatsApp and WeChat, which incorporate social media elements into private and group messaging. The future of social media appears to be headed towards more immersive experiences, such as the integration of virtual and augmented reality technologies. These developments suggest a continuing evolution of how social media platforms will be used for communication, business, and social interaction Each platform has tailored its features to fit specific audiences and usage styles, leading to a rich and varied social media ecosystem that continues to grow and evolve, impacting virtually every aspect of modern social interaction and communication.

How Social Media Shapes Perceptions and Behaviours

Social media significantly shapes perceptions and behaviors by serving as a primary platform for communication, information dissemination, and social interaction. It influences how individuals perceive themselves and others, molding societal norms and expectations through the content shared and interactions that occur. For example, exposure to curated lifestyles and idealized images can impact self-esteem and body image, leading individuals to aspire to unrealistic standards. Additionally, social media platforms are powerful tools for social and political mobilization, enabling users to organize, protest, and advocate for various causes rapidly and on a large scale. The echo chamber effect, where users are exposed primarily to information that aligns with their beliefs, can reinforce biases and influence voting behaviors and political opinions. Furthermore, the instant nature of social media can lead to impulsive behaviors and decision-making, as users are often prompted to react quickly to trending topics and viral content. Overall, social media profoundly affects individual and collective actions, shaping cultural trends and societal structures.

Social media significantly influences perceptions and behaviors regarding victim blaming and cyberbullying. Platforms often serve as amplifiers for these phenomena due to their vast reach and the anonymity they provide. In the context of victim blaming, social media can perpetuate harmful stereotypes and biases. For instance, when individuals share or comment on content related to incidents of aggression or harassment, the discourse may often shift towards scrutinizing the victim's actions rather than condemning the perpetrator's behavior. This can reinforce the notion that victims are somehow responsible for the harm inflicted upon them, thereby normalizing and entrenching victim blaming.

Similarly, the dynamics of cyberbullying are intensified by social media. The ease with which users can create and disseminate harmful content, coupled with the potential for anonymity, emboldens individuals to engage in aggressive behaviors without immediate repercussions. The public nature of these interactions can lead to a bandwagon effect, where others join in on the harassment, escalating the situation. Furthermore, the algorithms underlying social media platforms can inadvertently promote such content by prioritizing engagement, often at the cost of the well-being of individuals. Social media allows users to gauge others' opinions, which in turn shapes their own views and willingness to participate in discussions. This is often influenced by their fear of isolation or dissent, supporting theories like the spiral of silence, where individuals may refrain from expressing minority opinions to avoid social isolation.

These platforms, while connecting users and providing a space for expression, also have a dual role in influencing public opinion and behavior in complex and sometimes detrimental ways. This underscores the need for more robust moderation policies, user education, and legal frameworks to mitigate the adverse effects of social media on social behaviors like victim blaming and cyberbullying. The role of social media in cyberbullying is complex, with venues like Facebook and texting being common platforms. Perceptions of cyberbullying are influenced by the target's features, such as whether they are peers or celebrities, affecting the likelihood of bystander intervention.[49]

Social networks affect online behavior through social contagion effects, where users are influenced by the online actions and approvals (likes, shares) of their network. This influence is often stronger than the objective reality, indicating a significant impact of perceived social norms on behavior . social media significantly influences how victim blaming and bystander behaviors are manifested in cyberbullying scenarios. The online presentation and behavior of victims, along with the contexts of the interactions, play crucial roles in how others perceive and react to these incidents.

Characteristics Of Social Media That Facilitate Cyberbullying

Social media platforms, while offering vast opportunities for connectivity and expression, also present characteristics that can inadvertently facilitate cyberbullying. Understanding these

[49]Cybeurllying via social media | Elizabeth Whittaker | Request PDF. Available at: https://www.researchgate.net/publication/271672147_Cyberbullying_Via_Social_Media (Last visited 29 April 2024).

features is crucial in developing strategies to mitigate online harassment. Here are some key characteristics of social media that contribute to the occurrence of cyberbullying:

1. Anonymity- Many social media platforms allow users to create accounts with minimal verification of identity, enabling individuals to post or message anonymously. This anonymity can embolden users to engage in cyberbullying without fear of immediate repercussions or identification.
2. Accessibility - Social media is accessible 24/7 from virtually any internet-connected device. This constant accessibility means that individuals can perpetrate bullying at any time and victims can feel like there is no escape from the harassment, which can occur around the clock.
3. Virality- The structure of social media is designed to share content widely and quickly. Posts can go "viral" in a matter of hours, spreading hurtful or harmful messages to a large audience. This amplification can exacerbate the emotional impact on the victim.
4. Permanence- Once something is posted online, it can be difficult to completely erase. Even if original posts are deleted, copies may exist, or screenshots may have been taken. This permanence can prolong the distress caused by cyberbullying incidents.
5. Lack of Non-Verbal Cues- Social media communication lacks the non-verbal cues such as tone, facial expression, and body language that help convey context in face-to-face interactions. The absence of these cues can lead to misunderstandings and misinterpretations, allowing aggressive or harmful messages to be more easily disseminated.
6. Echo Chambers and Group Dynamics- social media often facilitates the formation of groups or communities that share similar interests or views. While generally positive, this clustering can also lead to "echo chambers" where groupthink can prevail, and dissenting opinions are ridiculed or targeted. Cyberbullies can leverage group dynamics to gang up on individuals, magnifying the effects of their actions.
7. Dehumanization- The digital nature of communication can lead to dehumanization, where users may not fully grasp the real-world impact of their words on another person’s emotions and mental health. This detachment can make it easier for some individuals to engage in cruelty they would not otherwise exhibit in person.
8. Platform Policies and Enforcement- Inconsistent enforcement of community guidelines and varying policies on what constitutes acceptable behavior can contribute to environments where cyberbullying thrives. When rules are not clearly defined or uniformly enforced, perpetrators may feel empowered to continue their behavior.

9. Rapid Technological Changes-The fast pace of technological innovation can sometimes outstrip a platform's ability to manage negative behaviors effectively. New features and tools can be exploited for harmful purposes before safeguards or moderation practices are fully developed.
10. Scale and Moderation Challenges- The sheer volume of content generated on social media platforms poses significant challenges for effective moderation. Automated systems and human moderators can struggle to keep up with the scale of data, leading to delays in addressing reported incidents of cyberbullying.

Social Media's Role in Propagating Victim Blaming

Social media plays a significant role in propagating victim blaming, particularly in cases of cyberbullying, harassment, and other forms of abuse. The interactive and highly public nature of social media platforms allows for the rapid spread of narratives that can unfairly blame victims for their own victimization. Comments, shares, and reactions can quickly amplify messages that question the credibility, behavior, or choices of victims, often under the guise of public opinion or debate[50]. This can lead to a culture where victims feel re-victimized and stigmatized, deterring them from coming forward or seeking help. The anonymity offered by social media can exacerbate this issue, as users may feel emboldened to express harsh or judgmental opinions without accountability. Furthermore, the echo chamber effect, where users are predominantly exposed to viewpoints like their own, can reinforce and validate victim-blaming attitudes, making them more pervasive. As such, social media not only spreads but can also validate and entrench harmful attitudes toward victims, making it a potent force in the persistence of victim blaming in society.

Legal Responsibilities of Social Media Platforms

In India, the legal responsibilities of social media platforms are primarily governed by the Information Technology (IT) Act, 2000, and its amendments, along with various guidelines and rules issued under its framework. As the digital landscape continues to evolve, so too do the regulations that ensure these platforms operate within legal boundaries while respecting users' rights.

Intermediary liability protection[51] is a critical aspect of the legal framework that governs social

[50] Carlyle, Kellie. (2017). The role of social media in promoting understanding of violence as a public health issue. Journal of Communication in Healthcare. 10. 1-3. 10.1080/17538068.2017.1373907. (Last visited 29 April 2024).
[51] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code)Rules, 2021

media platforms and other online intermediaries in India. This principle is embedded in the Information Technology (IT) Act, 2000, and further detailed in subsequent amendments and rules, notably the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

According to section 2(1)(w) of the IT Act[52], "Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes.

The concept of safe harbour is the legal foundation that shields intermediaries from being liable for the content generated by their users. The rationale behind this protection is to encourage the growth and development of the digital ecosystem by ensuring that platforms are not unduly burdened with the impossible task of monitoring every piece of content that passes through their systems. According to Section 79 of the IT Act[53], intermediaries are not liable for any third-party information, data, or communication link made available or hosted by them, provided they do not Initiate the transmission, Select the receiver of the transmission, and Select or modify the information contained in the transmission. The intent behind inserting section 79 is for providing safe harbour for intermediaries who should not held liable unreasonably. This protection is contingent on the intermediary's observance of due diligence while discharging its duties and upon following the guidelines prescribed by the government.

Due diligence requirements for social media platforms in India are specified under the Information Technology (IT) Act, 2000, particularly after the amendments introduced by the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 under Part 2 rule 3. These requirements are critical for maintaining the legal protection afforded by the safe harbor principles, which shield platforms from liabilities related to user-generated content. The due diligence requirements also aim to enhance accountability, ensure user safety, and promote ethical standards on digital platforms.

Publication and Clarity: Social media platforms are obligated to publish and make easily accessible their privacy policy, user agreement, and rules and regulations. These documents must be clear, concise, and transparent to ensure that users fully understand the terms of service and what is expected of them while using the platform. The policies must cover aspects such as data handling, user rights, and the types of permissible and prohibited activities.

[52] Information Technology Act, 2000, § 2(1)(w).
[53] Information Technology Act, 2000, § 79

Annual Notification: Platforms are required to notify users at least once per year about the rules and guidelines, emphasizing that non-compliance may lead to termination of access or other disciplinary actions. This regular communication is intended to keep users informed of their obligations and any updates to the policies, thus promoting a safe online environment.

Content of Policies: The privacy policy should detail how user data is collected, stored, used, and shared, including with third parties. It should also explain the measures taken to protect user privacy and data security. The user agreement and rules must clearly define acceptable and unacceptable behaviors on the platform, detailing the consequences of policy violations.

One of the cornerstone requirements is the establishment of an efficient and transparent grievance redressal mechanism. This system must be designed to address and resolve complaints from users regarding content that violates platform policies or legal provisions. Platforms are required to appoint a Grievance Officer whose contact details (name, contact number, and email address) must be prominently displayed on the platform. This officer is responsible for the redressal of user grievances. The Grievance Officer is tasked with acknowledging the receipt of any complaint within 24 hours and resolving it within 15 days from its receipt. This prompt response is crucial in addressing potentially harmful content swiftly and effectively. Platforms must keep records of all complaints received and the actions taken in response. They are also required to publish monthly compliance reports detailing the number of complaints received, resolved, and pending. This not only ensures transparency but also accountability to the public.

In summary, the due diligence requirements for social media platforms in India are designed to create a safer and more accountable online environment. However, the effectiveness of these regulations depends largely on their implementation, the platforms' commitment to these principles, and the evolving landscape of digital interactions and legal standards. As such, ongoing review and adaptation of these requirements are essential to keep pace with technological advancements and emerging online behaviours.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, introduced in India, establish specific mandates for social media platforms concerning the removal of unlawful content. This provision aims to balance the benefits of open digital communication with the need to prevent harm caused by illegal online activities.

The IT Rules 2021 mandate that social media platforms must remove or disable access to content deemed unlawful within 36 hours of receiving a court order or a notification from the appropriate government or its agency. This is a significant requirement aimed at ensuring that

harmful content does not remain accessible, potentially exacerbating the damage it may cause.

The definition of unlawful content includes, but is not limited to, materials that are explicitly sexual, libelous, hateful, or otherwise in violation of existing laws. This broad categorization ensures that various forms of harmful content are covered, including those that may incite violence, spread misinformation, or violate personal privacy.

Receiving Notifications: Social media platforms need to establish mechanisms to receive notifications of unlawful content from both courts and government agencies. This may involve designated points of contact or automated systems that can process such notifications efficiently.

Review and Action: Upon receiving a notification, the platform must promptly review the reported content against their policies and the specifics of the notification to determine the appropriate course of action. The requirement to act within 36 hours places significant pressure on platforms to have rapid response systems in place.

Challenges in Adjudication: Determining whether content is indeed unlawful can be complex, involving legal interpretations that may sometimes require platforms to make quasi-judicial decisions. This can be particularly challenging when the content is ambiguous or when it involves balancing freedom of expression against potential harm.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, introduced several stringent compliance requirements for significant social media intermediaries in India. These platforms, due to their large user base and potential impact on public discourse and security, are held to higher standards to ensure they act responsibly.

The requirement for traceability of originators aims to mitigate the misuse of social media platforms for spreading misinformation and other unlawful activities. Platforms are expected to develop capabilities to trace the "first originator" of information on their network. This does not necessarily mean tracking the content back to its creator but to the point where it entered the platform. This requirement raises significant concerns regarding user privacy and encryption, particularly in how platforms can implement this without breaking end-to-end encryption or compromising user confidentiality.

The Chief Compliance Officer (CCO) is tasked with ensuring the platform adheres to the IT Act and associated regulations, particularly regarding the management of content. This officer, typically with a background in legal or regulatory compliance, is crucial for overseeing legal compliance and is held accountable in any legal proceedings for failures in this area. Additionally, the Nodal Contact Person is responsible for continuous coordination with law enforcement agencies, managing legal requests and serving as the primary contact for law

enforcement across India, a role vital for addressing urgent national security threats or immediate harms. The Resident Grievance Officer plays a key role in maintaining user trust by managing and resolving user complaints about the platform's services, acknowledging complaints within 24 hours and resolving them within 15 days.

Platforms must publish reports every month detailing the complaints they have received and the actions they have taken in response. These reports are intended to provide transparency regarding the volume and types of issues handled and showcase the platform's responsiveness to concerns raised by users and authorities. The reports should be easily accessible to the public, often published on the platform's website.

Balancing Act - User Rights Vs. Regulatory Compliance

The obligation of social media platforms to adhere to regulatory compliance while simultaneously protecting user rights presents a complex balancing act. This intersection involves multiple facets, from ensuring user privacy and freedom of expression to aligning with legal and ethical standards imposed by governments[54].

Data Protection and Privacy: One of the primary concerns in the balance between user rights and regulatory compliance is the protection of user data. Platforms are expected to implement strong data protection measures that prevent unauthorized access and misuse of user information. This includes encryption, secure data storage solutions, and rigorous access controls. However, regulatory requirements such as the traceability of originators can conflict with these practices, particularly if they necessitate weakening encryption or increasing surveillance capabilities.

Transparency in Data Handling: Transparency about how user data is collected, used, and shared is crucial for maintaining user trust. Platforms must clearly communicate their data practices through privacy policies and user agreements and must obtain informed consent from users for the processing of their personal data.

Moderating Content: Social media platforms have the challenging task of moderating content to prevent illegal activities, hate speech, and misinformation while also protecting freedom of speech. Overly stringent content moderation policies might infringe on free expression, while lenient policies could allow harmful content to proliferate.

[54] Your virtual legal counsel. Available at: https://www.yvlc.legal/post/balancing-act-navigating-the-legal-landscape-of-social-media#:~:text=1.,privacy%20remains%20a%20critical%20issue. (last visited 29 April 2024).

Appeal Processes: Implementing fair and accessible appeal processes is vital. Users whose content has been removed or accounts have been suspended should have the right to understand why those actions were taken and to appeal against them if they feel they've been wrongly penalized.

Platforms must comply with local and international laws that govern online activities. This includes laws related to cyber security, data localization, and cooperation with law enforcement agencies. The challenge here is that laws can vary significantly across jurisdictions, making global operations particularly complex. Platforms often need to engage in dialogue with governments to shape and understand regulatory expectations. This relationship can be challenging, especially in countries where laws may be used to suppress dissent or limit free speech. Here, platforms must navigate the legal requirements while advocating for the protection of user rights.

Algorithms used for content moderation and ad targeting must be designed to avoid biases that could lead to discrimination. Ensuring algorithmic transparency and implementing regular audits can help address these issues. Social media platforms have a broader ethical responsibility to consider the societal impacts of their operations, including the mental health of users and the spread of misinformation. Balancing these concerns with business and regulatory pressures is increasingly important.

Engaging with users, civil society, and experts can provide valuable insights into how best to balance regulatory compliance with the protection of user rights. Developing internal policies that reflect a commitment to human rights, while still ensuring compliance with legal requirements, is essential. These policies should be adaptable to changing legal landscapes and societal expectations. Platforms need to be proactive in updating their practices in response to new legal developments, technological advancements, and evolving user expectations.

The balancing act between protecting user rights and complying with regulatory requirements is an ongoing challenge for social media platforms. This balance requires not only adherence to the law but also a strong commitment to ethical practices and respect for fundamental human rights. Achieving this balance is critical not only for legal compliance but also for maintaining user trust and the social legitimacy of these platforms.

Role Of Judiciary

The Indian judiciary plays a crucial role in addressing the issue of cyberbullying, particularly with respect to women on social media platforms. Through its interpretations of existing laws and the application of justice, the judiciary serves as a pivotal enforcer of legal

standards that protect individuals against cyberbullying. Indian courts rely on the Information Technology Act, 2000, particularly Section 67 which penalizes the publishing of obscene content online, and Section 79, which is pertinent to intermediaries like social media platforms, mandating them to exercise due diligence and swiftly remove unlawful content upon knowledge or notification.

Significantly, the judiciary also interprets the Indian Penal Code provisions that could apply to cyberbullying, such as Sections 354D (stalking), 499 (defamation), and 506 (criminal intimidation). In various rulings, courts have emphasized the responsibility of social media intermediaries to implement effective mechanisms for reporting and redressing grievances related to cyber harassment.

For example, in cases like Shreya Singhal v. Union of India, the Supreme Court has dealt with the balance between freedom of speech online and the suppression of online harassment, leading to the striking down of Section 66A of the IT Act, which was previously used to arrest individuals for online speech deemed annoying or offensive. The judiciary's decisions in these contexts not only refine the legal framework governing cyber conduct but also set precedents that shape the operational policies of social media companies in India, compelling them to be more vigilant and responsive to instances of cyberbullying.

By maintaining a stance that upholds both legal enforcement against cyberbullying and the protection of fundamental rights, the Indian judiciary contributes significantly to shaping a safer online environment for women. This judicial oversight ensures that social media intermediaries remain accountable, thereby mitigating the challenges posed by cyberbullying.

Shreya Singhal v. Union of India (2015)[55]- In this landmark judgment, the Supreme Court of India struck down Section 66A of the IT Act, 2000, which was often criticized for being misused to curb free speech on social media. The Court held that the section was unconstitutional as it was vague and overbroad.

Google India Pvt. Ltd. vs. Visaka Industries Limited (2019)[56]- This case dealt with the liability of online platforms for user-generated content. The Andhra Pradesh High Court held that intermediaries might be liable under certain circumstances if they have actual knowledge and have contributed to the commission of the unlawful act.

K.N. Govindacharya v. Union of India (2012)[57] – The Delhi High Court underscored the necessity for more stringent regulation of content on social media platforms, suggesting that

[55] AIR 2015 SUPREME COURT 1523
[56] Google India Private Ltd vs M/S. Visakha Industries on 10 December 2019, AIRONLINE 2019 SC 1708
[57] WP(C) 3672/2012

the government should ensure that these platforms do not become vehicles for illegal activities, and stressing the importance of accountability for content hosted on these platforms.

Taj Pharmaceuticals Ltd. v. Rajeshkumar Vishnubhai Patel & Ors. (2016)- The Bombay High Court in this case reaffirmed that intermediaries are generally protected from liability for third-party content as long as they comply with the due diligence requirements under the IT Act and do not play an active role in creating or modifying the content.

Amitabh Thakur v. Union of India (2016)[58] - This case highlighted the crucial role of social media in law enforcement. The Allahabad High Court examined the obligations of social media platforms to assist in preventing and investigating crimes, emphasizing that these platforms must cooperate with law enforcement agencies under certain circumstances to maintain public order and safety.

Kent RO Systems Ltd. & Anr. v. Amit Kotak & Ors (2017)[59] – This decision by the Delhi High Court clarified that intermediaries must exercise due diligence while discharging their duties under the IT Act and the Intermediary Guidelines. Failure to do so could strip them of the exemptions from liability traditionally granted under Section 79 of the IT Act.

Prajwala v. Union of India (2018)[60]- This case led to significant developments regarding the responsibilities of social media platforms in preventing the sharing of inappropriate content, including child pornography and videos related to sexual violence. The Supreme Court directed the setup of an online portal by the Union Government to receive complaints about such content.

Facebook Inc vs. Surinder Malik (2021)[61]- In this more recent case, the Delhi High Court discussed intermediary liabilities and emphasized the need for social media platforms to adhere to Indian laws, including providing information to law enforcement agencies when legally requested.

Union of India v. Twitter Inc. (2021)[62] - This recent case involved the Indian government directing Twitter to block accounts and tweets associated with certain hashtags related to farmer protests, raising significant questions about freedom of speech, government censorship, and the role of social media intermediaries in content governance.

These cases reflect the evolving legal landscape for social media intermediaries in India, balancing the need for regulation and the protection of free speech. The judiciary has actively

[58] Amitabh Thakur v. Union of India, (2016) 8 SCC 72
[59] Kent Ro Systems Ltd & Anr vs Amit Kotak & Ors on 18 January 2017 SCC Online Del. 7201.
[60] Prajwala v. Union Of India, AIR 2019 SC 162.
[61] Facebook Inc vs Surinder Malik & Ors on 28 August 2019 SCC Online Del 9887

interpreted these laws to ensure that social media platforms are held accountable for the content hosted on their services. Notably, Indian courts have emphasized the responsibility of intermediaries to act promptly upon complaints and to preserve the safety and dignity of users, particularly women who are victims of cyberbullying and harassment. For instance, in cases where intermediaries fail to comply with their obligations to protect users or remove harmful content, the judiciary has not hesitated to direct them to take specific actions, thereby reinforcing their role as gatekeepers of digital conduct.

CHAPTER-IV

COMPARATIVE REVIEW OF INTERNATIONAL LEGAL SYSTEMS

Comparative Analysis of Cyberbullying Laws

Cyberbullying represents a pervasive challenge in the digital age, affecting individuals across diverse demographics and national boundaries. As the internet continues to facilitate expansive social interactions, the instances of online harassment and bullying have escalated, prompting an urgent need for robust legal frameworks. Different countries have adopted varying approaches to tackle this issue, reflecting distinct cultural norms, legal traditions, and technological landscapes. This comparative analysis seeks to examine the cyberbullying laws across various countries to understand how legal definitions, enforcement mechanisms, and protective measures differ internationally. By scrutinizing the effectiveness of these laws in preventing and addressing cyberbullying, the study aims to highlight best practices and identify gaps in current legislation. This comparative perspective not only sheds light on the global efforts to combat cyberbullying but also offers insights into how legal systems can evolve to better protect individuals in a connected world. Through this analysis, we can explore the intricate balance between safeguarding personal rights and maintaining freedom of expression, crucial elements in crafting laws that are both effective and respectful of fundamental human rights.

I. Canada :

In Canada, cyberbullying is addressed through a combination of federal and provincial laws, reflecting the country's commitment to combating this pervasive issue. Canadian laws not only focus on the criminal aspects of cyberbullying but also include provisions for educational measures and civil remedies to protect victims. One of the pivotal moments in the legal landscape surrounding cyberbullying in Canada was the enactment of Bill C-13, also known as the Protecting Canadians from Online Crime Act, which came into force in March 2015.

Criminal Code of Canada

The Criminal Code has several provisions that can be applied to cyberbullying cases: Criminal Harassment (Section 264)[63]This section makes it illegal to engage in behavior that causes another person to fear for their safety. It covers repeated communication, including

[63] Criminal Code, RSC 1985, c C-46, s 264.

electronic communications, which can encompass cyberbullying. Uttering Threats (Section 264.1)[64]This includes conveying threats to cause death or bodily harm to any person, damage to property, or harm to animals. Intimidation (Section 423.1)[65] This section prohibits acts that compel a person to do (or abstain from doing) something they have a lawful right to do. Identity Fraud (Section 403)[66]This involves the fraudulent use of another person's identity information, relevant to cases where cyberbullies impersonate their victims online. Distribution of Intimate Images Without Consent (Section 162.1)[67] Enacted in March 2015, this law makes it a criminal offense to share intimate images of a person without that person's consent. This law directly addresses issues related to revenge porn, which often overlaps with cyberbullying.

Provincial Legislation

Various provinces in Canada have enacted their own laws to combat bullying and cyberbullying specifically - Nova Scotia: Following the high-profile *case of Rehtaeh Parsons*[68], Nova Scotia passed the Cyber-safety Act in 2013, although it was later struck down in 2015 due to concerns about its constitutionality. It was replaced by the Intimate Images and Cyber-protection Act in 2017, which allows victims to apply for protection orders and pursue lawsuits against perpetrators. Quebec's Act to Prevent and Stop Bullying and Violence in Schools requires school boards to implement anti-bullying plans, which include measures against cyberbullying. The Ontario's Accepting Schools Act requires schools to prevent and respond to bullying, including cyberbullying, as part of a safe and accepting school policy.

Canadian policy also emphasizes education and awareness as crucial components in combating cyberbullying. Various programs at the provincial level aim to educate both students and teachers on recognizing, preventing, and responding to cyberbullying incidents. Victims of cyberbullying in Canada can seek civil remedies including injunctions, restraining orders, or damages through civil suits, depending on the nature of the case and the harm suffered.

Bill C-13[69], the Protecting Canadians from Online Crime Act, introduced by the Canadian government and enacted on March 10, 2015, targets cyberbullying by amending various laws

[64] Criminal Code, RSC 1985, c C-46, s 264.1.
[65] Criminal Code, RSC 1985, c C-46, s 423.1.
[66] Criminal Code, RSC 1985, c C-46, s 403.
[67] Criminal Code, RSC 1985, c C-46, s 162.1.
[68] Independent Review of the Police and Prosecution Response to the Rehtaeh Parsons Case (last visited 12 May.2024)
[69] LegislativeSummaryforBillC-13.Availableat: https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/LegislativeSummaries/412C13E(last visited: 29 April 2024).

including the Criminal Code, the Canada Evidence Act, the Competition Act, and the Mutual Legal Assistance in Criminal Matters Act. Under these amendments, sharing intimate or sexual images of someone without their consent is considered a criminal offense, applicable not only to adults but also to individuals under 18 years old. Law enforcement can obtain warrants to access information about internet users suspected of committing cyberbullying-related offenses.

Cyberbullying, defined by the Government of Canada as deliberate, repeated, and hostile behavior using information and communication technologies to harm others, can overlap with online harassment. While cyberbullying typically involves intimidating and hurtful online actions among students, some actions can also constitute criminal harassment under section 264 of the Criminal Code Several high-profile incidents in Canada, particularly those involving the distribution of intimate images of young people or students, have heightened public awareness and pressured governments to address cyberbullying through legal means. Cyberbullying encompasses various actions such as posting embarrassing photos online, sending threatening messages, creating mocking websites, impersonating others, or tricking individuals into divulging personal information. Distributing intimate photos without consent carries severe penalties, with an 'intimate image' defined as one depicting explicit sexual activity, nudity, or sexual body parts, where the person depicted had a reasonable expectation of privacy.

An amendment to section 162.1 of the Criminal Code makes it an offense to publish an intimate image without consent, with penalties of up to five years in jail. Convicted individuals may also face additional consequences such as seizure of electronic devices used in the offense and reimbursement for the cost of removing the image from the internet. In cases where cyberbullying causes fear for safety, criminal harassment charges, punishable by up to 10 years in prison, may apply. Various other Criminal Code offenses such as uttering threats, intimidation, unauthorized computer use, mischief related to data, defamation, extortion, identity fraud, false messages, counseling suicide, and incitement of hatred may also be associated with online bullying depending on the nature of the actions.

In the 2016 trial of R v. Elliott, 2016 ONCJ 35: This case involved charges under the Criminal Harassment section of the Criminal Code, where the defendant was accused of engaging in a sustained campaign of harassing behavior towards two women on Twitter. The Ontario Court of Justice ultimately acquitted the accused, finding that the tweets did not constitute criminal harassment. This case highlighted the challenges of applying traditional harassment laws to online behavior. Although the prosecution established that the defendant's

tweets harassed the complainants, the trial judge dismissed the charges because there were no reasonable grounds to believe the complainants were genuinely afraid for their safety[70].

In this Ontario Superior Court case, the plaintiff was awarded damages for the intentional infliction of mental suffering and breach of privacy after the defendant posted an intimate video of her online without consent[71]. This case is significant because it addresses the non-consensual sharing of intimate images, which is often a component of cyberbullying.

In Canada, the approach to cyberbullying is encompassed within a broad legal framework that includes both criminal and civil law remedies. The government has taken steps to address the growing concerns related to online harassment and bullying, recognizing the severe impact these behaviors can have on victims.

II. United Kingdom

In the United Kingdom, the legal framework to combat cyberbullying against women is comprehensive, integrating both specific statutes and broader harassment and communication laws. This introduction to UK laws on cyberbullying against women provides an overview of how digital harassment is addressed, emphasizing the intersection of technology with gender-based violence. Cyberbullying, encompassing online threats, harassment, and the dissemination of private images without consent, is a significant concern that affects the safety and wellbeing of women. The UK's approach involves a combination of criminal sanctions, civil remedies, and protective measures designed to deter offenders and support victims.

The primary pieces of legislation include the Communications Act 2003, the Protection from Harassment Act 1997, and the Malicious Communications Act 1988. These laws are supplemented by recent updates such as the introduction of the Revenge Pornography Law under the Criminal Justice and Courts Act 2015. Together, they create a legal environment aimed at reducing cyberbullying and providing victims with necessary legal recourse. As digital platforms continue to evolve, UK law strives to adapt, ensuring robust protections for women against the growing threat of cyberbullying.

Communications Act 2003 –

Section 127[72]of the Communications Act 2003 in the UK addresses the issue of sending or causing to send messages through a "public electronic communications network" that are

[70] R. v. Elliott, 2016 ONCJ 35
[71] Doe 464533 v. N.D., 2016 ONSC 541
[72] Communications Act 2003, c. 21, § 127

grossly offensive, indecent, obscene, or menacing. This provision is particularly relevant in cases of cyberbullying, where individuals use electronic means to harass, intimidate, or threaten others. The law applies to messages sent through various electronic communication channels, including social media, email, and instant messaging. It aims to protect individuals from harmful or abusive online behavior and to maintain a safe and respectful online environment. In cases where a person is found guilty of violating Section 127, the punishment can include up to two years' imprisonment, a fine, or both. This demonstrates the seriousness with which the UK legal system views offenses related to cyberbullying and online harassment.

Section 127 is important in combating cyberbullying, especially when it targets vulnerable groups such as women. By criminalizing certain types of harmful online behavior, the law serves to deter individuals from engaging in cyberbullying and provides a means for victims to seek justice and protection.

DPP v. Collins [2006] UKHL 40- In this House of Lords case, the defendant was prosecuted under the Communications Act 2003 for making racially abusive telephone calls. The case highlighted the scope of what constitutes "grossly offensive" communication.

Chambers v DPP [2012] EWHC 2157 : Commonly known as the "Twitter Joke Trial[73]," this case involved a man who tweeted a joke about blowing up an airport. His conviction under the Communications Act 2003 was eventually quashed, raising important questions about the interpretation of "menacing" in online communications.

Protection from Harassment Act 1997-

The Protection from Harassment Act 1997 in the UK was initially enacted to address stalking but has since been extended to cover a wide range of behaviors, including cyberstalking and online harassment. The Act makes it an offense to pursue a course of conduct that amounts to harassment of another person and which the perpetrator knows or ought to know amounts to harassment. This can include persistent and unwanted contact via social media or other online platforms. The Act provides protection to individuals who are being targeted by harassment, whether in person or online. It recognizes the harmful impact that harassment can have on victims and seeks to provide them with legal recourse against perpetrators. Under the Act, a person convicted of harassment can face different penalties depending on the severity of the offense. On summary conviction (tried in a lower court), the punishment can include imprisonment for up to six months, a fine, or both. On conviction on

[73] R v Chambers, [2012] 1 WLR 3085

indictment (tried in a higher court), the punishment can be more severe, with the possibility of up to seven years' imprisonment.

The Protection from Harassment Act 1997 is an important tool in combating cyberstalking and online harassment, as it provides a legal framework for prosecuting offenders and protecting victims. It sends a clear message that such behavior is not acceptable and can have serious consequences.

Malicious Communications Act 1988-

The Malicious Communications Act 1988 in the UK is a law that specifically targets the sending of threatening, offensive, or otherwise malicious communications to another person. The Act covers a wide range of communications, including letters, electronic communications (such as emails, text messages, and social media posts), and articles of any description. Under this Act, it is an offense to send a communication that is indecent, grossly offensive, threatening, or false, with the intention of causing distress or anxiety to the recipient. The key element of the offense is the intent behind the communication; the sender must have intended to cause distress or anxiety to the recipient for the offense to be committed.

The Act recognizes the harm that can be caused by malicious communications, particularly in the context of modern technology and online communication. It provides a legal framework for prosecuting individuals who engage in this type of behavior, regardless of the medium used to send the communication. The penalties for offenses under the Malicious Communications Act 1988 can vary depending on the severity of the offense. In some cases, individuals convicted of offenses under this Act may face imprisonment, fines, or community service orders. The Act serves as a deterrent against sending malicious communications and helps to protect individuals from harassment, bullying, and other forms of abusive behavior.

Serious Crime Act 2015-

The Serious Crime Act 2015 in the UK introduced the offense of controlling or coercive behavior in an intimate or family relationship. This section of the Act recognizes that abuse and manipulation can occur in various forms beyond physical interactions, including through digital communications such as cyberbullying or online manipulations.

Controlling or coercive behaviour is defined as a pattern of behaviour that is used to harm, punish, or frighten a victim, and which may also include acts of assault, threats, humiliation, or intimidation. This behaviour can occur over time and can have a serious impact on the victim's physical, emotional, and psychological well-being. In the context of digital

communications, controlling or coercive behaviour can manifest in various ways, such as monitoring or controlling a victim's online activities, using social media or messaging apps to harass or intimidate, or spreading false information or rumors to manipulate or control the victim.

Section 76 of the Serious Crime Act 2015[74] recognizes the evolving nature of relationships and the ways in which abuse and manipulation can occur in the digital age. By including digital communications within the scope of controlling or coercive behavior, the Act provides a legal framework for prosecuting individuals who engage in such behavior, regardless of the medium used. The implications of this section extend beyond physical relationships to encompass online behaviors that can have a profound impact on victims. It sends a clear message that controlling or coercive behaviour, whether offline or online, is not acceptable and will be treated as a serious offense under the law. The UK's approach emphasizes both criminal sanctions and civil remedies to combat cyberbullying, and there has been significant discussion about the need for specific laws that address the unique challenges posed by cyberbullying.

III. Australia

In Australia, the legal framework addressing cyberbullying, particularly against women, reflects a comprehensive approach integrating both criminal and civil remedies. This framework is informed by a recognition of the serious impact that online harassment can have on individuals, particularly women, who are often disproportionately targeted by such behavior.

Criminal Code Act 1995 (Commonwealth):

Section 474.17 specifically addresses the use of a carriage service (which includes the internet and telecommunications services) to menace, harass, or cause offense. This section is often used to prosecute cases of cyberbullying, including those targeting women.

Under Section 474.17[75], it is an offense to use a carriage service in a way that reasonable persons would regard as being menacing, harassing, or offensive. This can include sending threatening or abusive messages, posting harmful or derogatory content online, or engaging in other forms of online behavior that are intended to harm or intimidate another person. The offense is broad in scope and can cover a wide range of behaviors that constitute cyberbullying. It recognizes the serious impact that cyberbullying can have on victims and aims to deter

[74] Serious Crime Act 2015, c 9, § 76.
[75] Criminal Code Act 1995 (Cth) s 474.17.

individuals from engaging in this type of behavior. Penalties for offenses under Section 474.17 can vary depending on the severity of the conduct and the harm caused to the victim. In some cases, individuals convicted of this offense may face imprisonment, fines, or other penalties.

The inclusion of provisions like Section 474.17 in the Criminal Code Act 1995 highlights the importance of addressing cyberbullying as a serious issue that can have legal consequences. It provides a legal framework for prosecuting offenders and seeking justice for victims of cyberbullying, including women who may be disproportionately targeted.

Each Australian state and territory have its own criminal laws which may apply to cyberbullying. For example, stalking, harassment, and threats are criminalized in all jurisdictions, and these laws can cover actions conducted via digital platforms.

The Enhancing Online Safety Act 2015:

This Act established the Office of the eSafety Commissioner, the first of its kind globally, with broad powers to promote online safety. This includes handling complaints about cyberbullying and having the authority to direct internet service providers to remove content deemed as cyberbullying. Specific provisions for Image-based Abuse: Often targeting women, the sharing of intimate images without consent is directly addressed under both federal and state laws. The eSafety Commissioner has specific powers to take expedited action in cases of non-consensual sharing of intimate images.Victims of cyberbullying can also seek civil remedies which can include injunctions to prevent further harassment or defamation actions, depending on the nature of the bullying.

Dow Jones & Co Inc. v Gutnick (2002) 210 CLR 575:

While primarily concerning defamation, this High Court of Australia case is significant for establishing jurisdictional issues related to online activities. It affirmed that online actions causing harm in Australia can be subject to Australian law, relevant to cyberbullying cases where international elements are involved.

IV. New Zealand

In New Zealand, the approach to combating cyberbullying is comprehensive and structured, particularly under the Harmful Digital Communications Act (HDCA), which came into force in 2015. This legislation was specifically designed to address issues related to digital communication, including cyberbullying, and provides a clear legal framework to deal with such incidents effectively.

Harmful Digital Communications Act 2015 –

The HDCA sets out principles and creates offenses specifically aimed at reducing harm caused by digital communications, including cyberbullying. The Act focuses on behavior that seriously breaches these principles through digital means. The Act establishes ten communication principles that apply to digital communications, including that a communication should not disclose sensitive personal facts about another person, should not be threatening, offensive, or indecent, and should not be used to harass an individual.

Director of Human Rights Proceedings v. Jefferies [2020] NZHRRT 19: This case involved offensive and racist tweets directed at the Mayor of Wellington. The Human Rights Review Tribunal found these communications breached the HDCA. The decision emphasized that the HDCA could apply to public figures and addressed the intersection of freedom of expression and harmful digital communications.

Police v. B [2017] NZYC 174: In this Youth Court case, a young person was charged under the HDCA for posting a digitally altered, indecent image of a school teacher on social media. The case highlighted the application of the HDCA in protecting individuals from malicious digital content intended to cause harm.

Victims of cyberbullying can file a complaint with the approved agency (NetSafe), which provides advice and mediation services. If NetSafe's mediation fails, the case can be taken to the District Court, which has a range of orders it can issue, such as take-down orders for content, cease-and-desist orders, and orders to release the identity of anonymous offenders.

The Act includes provisions for criminal proceedings against those who commit serious offenses under the Act, with penalties including fines and imprisonment. For example, causing harm by posting digital communication can result in up to two years' imprisonment or a fine up to NZD $50,000 for individuals, and up to NZD $200,000 for body corporates.

V. USA:

Cyberbullying in the U.S. is addressed through a combination of federal and state laws, as well as specific policies implemented by schools and other institutions. There is no single federal statute specifically dedicated to cyberbullying, but several federal laws are applied to cases of cyberbullying:

Civil Rights Act of 1964:

This act is used in cases where cyberbullying involves discrimination based on race, color, national origin, sex, or disability. The Civil Rights Act of 1964 primarily focuses on prohibiting

discrimination based on race, color, religion, sex, or national origin in various aspects of public life. While it does not directly address cyberbullying, it has been used in some cases to address harassment or discrimination that occurs online, particularly when it intersects with issues of race, sex, or religion.

For example, Title VII of the Civil Rights Act, which deals with employment discrimination, has been cited in cases where cyberbullying or harassment in the workplace is based on protected characteristics such as race or gender. Additionally, Title IX, which prohibits sex discrimination in education, has been invoked in cases of cyberbullying or harassment in educational settings. While the Civil Rights Act of 1964 may not directly address cyberbullying as a standalone issue, its provisions against discrimination have been applied in certain contexts to address online harassment that is based on protected characteristics.

Children's Internet Protection Act (CIPA) of 2000:

The Children's Internet Protection Act (CIPA) of 2000 is a United States federal law aimed at protecting children from accessing harmful online content. It requires schools and libraries that receive federal funding for internet access to implement measures to filter or block obscene or harmful content, as well as to educate minors about appropriate online behavior. While CIPA is primarily focused on protecting children from inappropriate content and promoting online safety, it does not specifically address cyberbullying. However, the law's emphasis on promoting safe and responsible internet use for children aligns with broader efforts to address cyberbullying and online harassment among young people. Schools and libraries covered by CIPA are often key stakeholders in implementing policies and programs to prevent and address cyberbullying among students.

Violence Against Women Reauthorization Act of 2013:

The Violence Against Women Reauthorization Act of 2013 (VAWA 2013) is a United States federal law that reauthorized and expanded the original Violence Against Women Act (VAWA) of 1994. While VAWA primarily focuses on combating domestic violence, dating violence, sexual assault, and stalking, it also includes provisions that are relevant to cases of cyber-stalking, which can overlap with cyberbullying. Under VAWA 2013, the definition of stalking includes "conduct that causes substantial emotional distress" or "fear of death or serious bodily injury." This broad definition can encompass a range of behaviors, including cyber-stalking, which involves the use of electronic communications to harass or intimidate an individual. VAWA provides resources and support for victims of stalking, including those who

experience cyber-stalking, and encourages law enforcement agencies to take these crimes seriously. While VAWA 2013 does not specifically mention cyberbullying, the provisions related to stalking can be applicable in cases where cyberbullying involves persistent and targeted harassment or intimidation. Additionally, VAWA's emphasis on supporting victims and holding perpetrators accountable aligns with efforts to address cyberbullying and other forms of online harassment.

Additionally, most U.S. states have laws that specifically address bullying and cyberbullying. These laws often require schools to have policies against bullying, which include cyberbullying, and may provide for various penalties or required interventions. Some state laws explicitly include electronic forms of communication within their definitions of bullying. For instance, California's Safe Place to Learn Act extends protections against bullying to include electronic acts acts that are committed through devices or systems like social media. New York has the Dignity for All Students Act, which addresses harassment and bullying within the school environment, including cyberbullying. Each state has its own statutes, so the specifics can vary widely depending on the jurisdiction in question. If you need information about a specific state's laws or further details on federal statutes, please provide the jurisdiction or additional details.

Comparative Analysis-

The comparative analysis of cyberbullying laws across different countries namely the United Kingdom, the United States, India, Canada, and Australia reveals varied approaches based on cultural, legal, and technological contexts. In the United Kingdom, there is no standalone law for cyberbullying; instead, it is addressed under multiple acts that cover broader aspects of communication and harassment, such as the Communications Act 2003 and the Malicious Communications Act 1988. This approach emphasizes criminal behaviors that can lead to prosecution and integrates policies within educational settings for minors.Contrastingly, the United States lacks a unified federal law, leading to a diverse landscape of state-level legislation. States independently define and regulate cyberbullying, resulting in a patchwork of laws. For example, New York's Dignity for All Students Act explicitly includes provisions against cyberbullying, demonstrating a proactive stance at the state level. India's strategy involves incorporating cyberbullying under the umbrella of the Information Technology Act, 2000, with specific criminal provisions found in the Indian Penal Code, like sections 507 and 509.

The striking down of Section 66A by the Supreme Court in 2015 for vagueness and

unconstitutionality marked a significant judicial response to concerns about freedom of speech, thus influencing how cyberbullying is legislated. Canada employs a dual approach using both criminal law and provincial educational policies to combat cyberbullying. The Criminal Code addresses various aspects of cyberbullying through provisions like defamatory libel and harassing communications. Additionally, provincial legislation mandates that schools have anti-cyberbullying policies, which demonstrates a commitment to both punitive and preventative measures.

Australia stands out by having both national and state-specific legislation, coupled with the establishment of the Office of the Safety Commissioner under the Enhancing Online Safety Act 2015. This body plays a significant role in promoting online safety and directly tackling cyberbullying, showcasing an institutional commitment to combating cyberbullying with dedicated resources. In conclusion, while all these countries recognize the severity of cyberbullying, their legislative responses vary widely. From broad applications of general laws to specific statutes and dedicated governmental bodies, each approach provides insights into the multifaceted strategies needed to effectively address cyberbullying in the digital age.

Comparative Analysis of Social Media Regulations

I. USA

Social media regulations in the USA are primarily governed by a combination of federal laws, state-specific statutes, and self-regulation by the platforms themselves. Here are some of the key federal laws that impact social media operations, along with their specific provisions:

Communications Decency Act (CDA) of 1996:

Section 230 of the Communications Decency Act (CDA) of 1996 is a crucial piece of legislation that provides immunity to online platforms, including social media companies, from being held liable for the content posted by their users. This immunity is a key factor that has allowed social media platforms to thrive and host user-generated content without fear of legal repercussions.

Section 230 states, in part, that *"No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."* This provision shields online platforms from being held liable for content posted by users, with some exceptions, such as intellectual property violations and certain criminal acts. Section 230 also provides platforms with the flexibility to moderate and remove content that they deem objectionable, without being seen as engaging in editorial control.

However, platforms are required to act in "good faith" when moderating content, meaning they must not be acting with the intent to silence specific viewpoints or engage in unfair or deceptive practices. Overall, Section 230 has been instrumental in shaping the modern internet landscape, allowing for the growth of user-generated content platforms while also raising questions about the balance between freedom of expression and the regulation of harmful content online.

Children's Online Privacy Protection Act (COPPA) of 1998:

The Children's Online Privacy Protection Act (COPPA) of 1998 is a United States federal law that regulates the online collection of personal information from children under the age of 13. COPPA requires website operators and online service providers to obtain verifiable parental consent before collecting, using, or disclosing personal information from children.

Under COPPA, personal information includes a child's name, address, email address, telephone number, and any other information that can be used to identify or contact a child online. The law also requires operators to post clear privacy policies and provide parents with the ability to review and delete their child's information. COPPA imposes strict requirements on operators of websites and online services that are directed at children or have actual knowledge that they are collecting personal information from children. Failure to comply with COPPA can result in significant fines and penalties. Overall, COPPA is designed to protect the privacy and safety of children online by regulating how their personal information is collected, used, and disclosed by websites and online services.

Electronic Communications Privacy Act (ECPA) of 1986:

The Electronic Communications Privacy Act (ECPA) of 1986 is a United States federal law that sets out the rules for how electronic communications, such as emails, phone calls, and data transmissions, can be intercepted, accessed, and disclosed by third parties. ECPA includes provisions that protect the privacy of electronic communications while they are being transmitted, in storage, and when they are discarded. These provisions require government entities to obtain a warrant in order to intercept or access the contents of electronic communications, with some exceptions for certain types of communications and circumstances.

Social media platforms and other online service providers must comply with ECPA to ensure the privacy and security of user communications. This includes protecting the confidentiality of communications in transit and implementing security measures to prevent unauthorized access to user data. ECPA has been the subject of ongoing debate and criticism,

particularly regarding its application to modern forms of communication such as email and social media. Some argue that ECPA is outdated and in need of reform to better protect privacy in the digital age.

In addition to federal laws, states like California have enacted their own regulations, such as the California Consumer Privacy Act (CCPA), which gives consumers more control over the personal information that businesses collect about them. This law affects social media companies that collect data from California residents. These regulations reflect the complex environment in which social media operates, balancing the protection of user rights with fostering innovation and free expression.

Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC (2008):

This case challenged the immunity under Section 230 of the CDA, where the Ninth Circuit held that Roommates.com was not entitled to immunity because it contributed to the development of the illegal content by requiring users to provide discriminatory preferences in housing postings.

Packingham v. North Carolina (2017)[76]: The Supreme Court struck down a North Carolina law that restricted registered sex offenders from accessing social media sites. The Court ruled that this law violated the First Amendment's free speech clause.

Lorenzo v. Securities and Exchange Commission (2018): This case dealt with the dissemination of false statements on social media and its implications under securities fraud laws. The Supreme Court held that dissemination of knowingly false statements, even without "making" the statement directly, can lead to liability.

II. Australia

Australia has implemented several laws aimed at regulating social media use and protecting users from online harms:

Enhancing Online Safety Act 2015:

The Enhancing Online Safety Act 2015 in Australia is a significant piece of legislation aimed at improving online safety for Australians. One of its key provisions was the establishment of the Office of the eSafety Commissioner, making it the world's first government agency dedicated solely to online safety.

[76] 582 U.S. 98 (2017)

The eSafety Commissioner is empowered by the Act to enforce regulations that protect Australians, particularly children and young people, from online harms such as cyberbullying, online abuse, and inappropriate content. The Commissioner has the authority to investigate complaints, issue takedown notices for harmful online content, and provide advice and support to individuals, schools, and organizations on online safety issues.One of the important aspects of the Act is the provision for a complaints system specifically for young Australians who experience serious cyberbullying. This system allows young people, or their representatives, to make a complaint to the eSafety Commissioner about harmful online content. The Commissioner can then take action to have the content removed or blocked, and provide support to the victim.

The Act also includes provisions for education and awareness programs to promote online safety and digital literacy among Australians. These programs aim to empower individuals to protect themselves online and make informed decisions about their online activities. Overall, the Enhancing Online Safety Act 2015 is a comprehensive piece of legislation that seeks to address the complex challenges of online safety in the digital age. By establishing the eSafety Commissioner and providing mechanisms to address online harms, the Act plays a crucial role in protecting Australians, particularly young people, from the negative impacts of online abuse and cyberbullying.

Privacy Act 1988:

The Privacy Act 1988 in Australia is a crucial piece of legislation that governs the handling of personal information by social media platforms and other entities. It aims to protect individuals' privacy by regulating the collection, use, and disclosure of personal information. One of the key aspects of the Privacy Act relevant to social media platforms is the Australian Privacy Principles (APPs). These principles set out the standards, rights, and obligations for handling personal information. They cover a range of areas including the collection of personal information, the use and disclosure of personal information, data security, and the access and correction of personal information.

For social media platforms, the APPs require that they have a clear and transparent privacy policy that explains how they collect, use, and disclose personal information. This includes information about the types of personal information collected, the purposes for which it is collected, and how individuals can access and correct their information.

The Privacy Act also requires that social media platforms take reasonable steps to protect the personal information they hold from misuse, interference, and loss, as well as unauthorized

access, modification, or disclosure. This includes implementing security measures such as encryption, access controls, and regular security audits.

In addition, the Privacy Act gives individuals the right to access and correct their personal information held by social media platforms. Individuals can also make complaints to the Office of the Australian Information Commissioner (OAIC) if they believe that a social media platform has breached the Privacy Act. Overall, the Privacy Act 1988 and the Australian Privacy Principles play a crucial role in regulating the handling of personal information by social media platforms, ensuring that individuals' privacy rights are protected in the digital age.

Australia has also proposed or enacted specific legislation in response to contemporary issues, such as the Online Safety Act 2021, which aims to further enhance the powers of the eSafety Commissioner and extend regulations to a broader spectrum of online harms. These laws collectively form a robust framework intended to regulate social media platforms, protect individual privacy, and combat online harms.

III. Canada

Canadian social media regulation primarily falls under federal and provincial privacy laws, anti-spam legislation, and specific laws targeting harmful online content. Here are some of the main legislative frameworks:

Personal Information Protection and Electronic Documents Act (PIPEDA):

The Personal Information Protection and Electronic Documents Act (PIPEDA) is the federal privacy law in Canada that governs how private-sector organizations collect, use, and disclose personal information in the course of commercial business. PIPEDA applies to organizations engaged in commercial activities across Canada, with some exceptions in certain provinces that have their own substantially similar legislation.

Under PIPEDA, social media platforms are considered private-sector organizations and are therefore subject to its provisions. This means that social media platforms must comply with PIPEDA when collecting, using, or disclosing personal information of their users. One of the key principles of PIPEDA is the requirement for organizations to obtain meaningful consent for the collection, use, and disclosure of personal information. This means that social media platforms must clearly explain to users why their personal information is being collected, how it will be used, and with whom it may be shared. Users must then be given the opportunity to consent to or refuse the collection, use, or disclosure of their personal information. PIPEDA also requires organizations to protect the personal information they collect by implementing

appropriate security measures. This includes safeguards against unauthorized access, disclosure, copying, use, or modification of personal information.

Additionally, PIPEDA gives individuals the right to access and request corrections to their personal information held by an organization. Individuals also have the right to file a complaint with the Office of the Privacy Commissioner of Canada if they believe their privacy rights under PIPEDA have been violated.

Canada's Anti-Spam Legislation (CASL):

Canada's Anti-Spam Legislation (CASL) is a law that aims to control spam and other electronic threats, such as phishing, malware, and spyware. One of the key aspects of CASL is that it requires businesses to obtain consent before sending commercial electronic messages (CEMs), including emails, texts, and certain social media messages, to Canadian recipients.

In the context of social media, CASL impacts how companies engage with users regarding advertising and marketing. For example, if a business wants to send promotional messages or sponsored content to users on social media platforms, they must ensure that they have obtained the necessary consent from Canadian users before doing so. This means that businesses cannot send unsolicited commercial messages to Canadian users without their consent, even if the messages are sent through social media platforms. CASL also requires that all CEMs include certain identification information about the sender, as well as a way for recipients to unsubscribe from receiving future messages. This unsubscribe mechanism must be easy to use and must be functional for at least 60 days after the message is sent.

In relation to cyberbullying, CASL may indirectly play a role in preventing the spread of harmful electronic messages. While CASL primarily focuses on commercial messages, the requirement for consent and the prohibition of unsolicited messages can help deter individuals from sending harassing or abusive messages through electronic means, including social media platforms. CASL is an important piece of legislation that helps protect Canadians from unwanted electronic messages and threats, and it also has implications for how businesses engage with users on social media regarding advertising and marketing.These laws and proposed changes highlight Canada's approach to regulating social media platforms, focusing on privacy, consent, protection from harassment, and the promotion of safe digital spaces. Each piece of legislation targets different aspects of social media use and has different implications for users and providers.

IV. China

Social media regulation in China is characterized by strict and comprehensive control by the government, with multiple laws and regulations designed to monitor and govern the operation of social media platforms and online behavior. Here are the key aspects of social media regulation in China:

Data Security Law (2021):

The Data Security Law of China, enacted in 2021, complements the Cybersecurity Law by setting out stricter requirements for the handling of data, particularly data affecting China's national security. The law applies to all entities, including social media companies, that collect, process, use, transmit, or store data within China. One key aspect of the Data Security Law is the requirement for social media companies and other entities to undergo periodic data security assessments and submit reports to authorities. These assessments are intended to identify and mitigate risks to data security, including risks related to cyberbullying and other forms of online harassment.

By requiring social media companies to assess and report on data security risks, the Data Security Law aims to enhance the protection of personal data and national security interests. This could have implications for addressing cyberbullying by ensuring that social media platforms have robust data protection measures in place to prevent the misuse of personal data for harmful purposes. the Data Security Law complements existing cybersecurity and data protection laws in China by providing additional requirements and safeguards to protect data, including data that may be relevant to cyberbullying incidents.

Provisions on the Governance of the Online Information Content Ecosystem (2020):

The Provisions on the Governance of the Online Information Content Ecosystem, issued in 2020, categorize online content into "encouraged," "negative," and "illegal" content categories. These rules explicitly require online platforms to manage and censor content that disrupts social order or is politically sensitive.

Under these provisions, online platforms are responsible for monitoring and managing the content posted by users to ensure that it complies with the categories outlined. Content that is deemed "encouraged," such as content that promotes positive social values or economic development, is allowed and may even be promoted by platforms. However, content categorized as "negative," which includes content that disrupts social order or undermines societal values, must be managed and, if necessary, censored by platforms. Similarly, content

categorized as "illegal," such as content that violates laws or regulations, must be promptly removed by platforms.

These rules have significant implications for addressing cyberbullying, as they empower online platforms to take action against content that is harmful or abusive. By categorizing and regulating online content, the rules aim to create a more positive and harmonious online environment, which could help in reducing incidents of cyberbullying.

However, there are concerns that these rules could also be used to suppress freedom of expression and stifle dissenting opinions, as platforms may be inclined to censor content that is politically sensitive or critical of the government. Additionally, there are challenges in effectively implementing and enforcing these rules, particularly given the vast amount of content generated online and the difficulty in accurately categorizing and moderating it.Overall, while the Provisions on the Governance of the Online Information Content Ecosystem aim to promote a healthier online environment, they also raise important questions about censorship, freedom of expression, and the role of online platforms in regulating content.

Real-Name Registration Rules:

The Real-Name Registration Rules in China, initiated in 2012 and strengthened over the years, require users to register for social media platforms using their real names. While users can still use usernames publicly, their real identities are linked to their accounts, allowing for easier monitoring and control by authorities.

These rules are part of China's broader efforts to regulate the internet and ensure the safety and security of its citizens online. By requiring real-name registration, the government aims to promote accountability and deter illegal or harmful online behavior, including cyberbullying. From the perspective of addressing cyberbullying, real-name registration can serve as a deterrent, as individuals may be less likely to engage in abusive behavior if their real identity is tied to their online actions. It also enables authorities to track and identify individuals who engage in cyberbullying, allowing for swifter and more effective enforcement actions more easily.

However, critics argue that real-name registration may also stifle freedom of expression and privacy rights, as individuals may feel constrained in expressing their opinions online if they fear repercussions for doing so. Additionally, there are concerns about the potential for misuse. While real-name registration rules in China may help in addressing cyberbullying by promoting accountability and enabling better monitoring, they also raise important questions about the balance between security and privacy, and the impact on freedom of expression

online[77].

Social media platforms operating in China, including local companies like Weibo, Tencent (WeChat), and ByteDance (TikTok/Douyin), as well as any foreign platforms attempting to enter the market, must comply with these regulations. They are responsible for content moderation according to government guidelines and face severe penalties for non-compliance, including fines and potential revocation of operating licenses.

China's approach reflects its broader governance and control objectives, ensuring that social media serves as an extension of state surveillance and propaganda apparatus, rather than as platforms for unfettered public discourse.

Comparative Analysis-

Social media regulations demonstrate considerable variation globally, largely influenced by differing legal structures and cultural priorities. This comparative analysis will explore how these regulations manifest in the U.S., China, and India, providing a clear perspective on their respective approaches. In the United States, social media regulation is characterized by its relatively lenient stance, rooted in the constitutional right to freedom of speech. Unlike other countries, the U.S. lacks a dedicated federal statute that directly governs social media platforms. Instead, existing legislations such as the Communications Decency Act, particularly Section 230, shield these platforms from being liable for user-posted content. This approach underlines the U.S. preference for minimal governmental intervention in online speech, although specific aspects like user privacy are addressed through targeted laws such as the Children's Online Privacy Protection Act (COPPA).

Contrastingly, China employs one of the most rigorous social media regulatory frameworks worldwide. The government maintains strict oversight over the internet, actively censoring any content deemed as potentially destabilizing or critical of the state. The Cyberspace Administration of China plays a pivotal role in enforcing these regulations. Social media companies in China are not only required to filter and censor content but also to actively monitor and report on the interactions that occur on their platforms, ensuring nothing contravenes the state’s directives on maintaining social harmony.

India's approach to social media regulation is more dynamic, reflecting its evolving policy landscape. The recent Information Technology (Guidelines for Intermediaries and Digital

[77] Lee, Yh-An & Liu, Ching-Yi. "Real-Name Registration Rules and the Fading Digital Anonymity in China," 25 Wash.Int'lL.J.1(2016),availableat_https://digitalcommons.law.uw.edu/wilj/vol25/iss1/3. (Last visited at 15. May 2024)

Media Ethics Code) Rules of 2021 exemplify this transition. These rules mandate that social media platforms remove any content that could threaten the nation's sovereignty, security, or public order. Additionally, significant social media entities are compelled to establish a physical presence in India, likely aimed at facilitating better compliance and accountability. The introduction of a grievance redressal mechanism further underscores India's commitment to more structured regulation, balancing governmental control with user engagement.

This comparative analysis reveals a spectrum of regulatory frameworks, from the U.S.'s focus on protecting freedom of expression to China's stringent controls and India's developing regulatory environment. Each approach reflects broader national priorities whether they prioritize individual rights, state control, or are transitioning towards more comprehensive oversight mechanism.

CHAPTER-V

GENDER, TECHNOLOGY, AND LAW: NAVIGATING CYBERBULLYING LAWS IN INDIA

Balancing the freedom of expression and the right to privacy on social media, especially in relation to cyberbullying cases, presents a complex and evolving legal challenge. The advent of digital communication platforms has exponentially increased the opportunities for free expression but has also raised significant concerns regarding personal privacy. Freedom of expression is a fundamental right safeguarded by numerous international and national legal frameworks, allowing individuals to share ideas and information without undue government restriction. Conversely, the right to privacy protects individuals from unwarranted intrusion into their personal life, a boundary that is frequently tested in the digital age.

Social media platforms, serving as the modern public square, often find themselves at the intersection of these conflicting rights. In the context of cyberbullying, the exercise of free speech can sometimes cross into abusive behavior, leading to severe emotional and psychological harm. This introduces legal complexities as jurisdictions strive to protect individuals from harassment while safeguarding the freedom of speech. The challenge for lawmakers and courts lies in defining the thresholds at which the harmful effects of cyberbullying override the general principle of free expression. Legal measures, such as anti-cyberbullying laws and regulations designed to protect personal data, must be carefully crafted to avoid encroaching on the freedom of expression while providing real protections that deter privacy violations. This delicate balance demands a nuanced understanding of both rights and their implications in the digital realm, emphasizing the need for legal frameworks that adapt to the evolving nature of communication and privacy concerns on social media platforms.

Definitions of Freedom of Expression and Right to Privacy.

Freedom of expression and the right to privacy are cornerstone human rights recognized by various international legal instruments.

I. Universal Declaration of Human Rights (UDHR)

The Universal Declaration of Human Rights (UDHR) enshrines the rights to freedom of expression and privacy as fundamental human rights. Freedom of expression, as articulated in Article 19 of the UDHR[78], is crucial for the development of democratic societies. It allows

[78]Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/RES/217(III) (Dec. 10, 1948), art.19.

individuals to express their thoughts, opinions, and ideas freely, without fear of censorship or reprisal. This right extends to all forms of media and communication, highlighting its broad scope and importance in the digital age.

The right to privacy, as stated in Article 12 of the UDHR[79], protects individuals from unwarranted intrusions into their personal lives. It encompasses not only physical spaces such as the home, but also extends to personal communications and reputation. This right ensures that individuals can maintain autonomy over their personal information and decisions.

In the context of social media and cyberbullying, these rights remain relevant and applicable. Individuals should be able to express themselves online without fear of harassment or intimidation. At the same time, they should also have the right to protect their personal information and reputation from malicious attacks. Balancing these rights is essential in ensuring a safe and inclusive online environment.

II. International Covenant on Civil and Political Rights (ICCPR)

The International Covenant on Civil and Political Rights (ICCPR) outlines fundamental rights and freedoms that apply to all individuals. Article 19 of the ICCPR guarantees the right to freedom of expression[80]. This right encompasses the freedom to seek, receive, and impart information and ideas through any medium, including oral, written, or artistic forms. Importantly, this right extends across borders, meaning that individuals have the right to access and share information globally.

Article 17 of the ICCPR establishes the right to privacy[81]. It states that no one should be subjected to arbitrary or unlawful interference with their privacy, family, home, or correspondence. Additionally, individuals have the right to be protected by the law against such interference or attacks on their honor and reputation.

These rights are essential in the context of social media and cyberbullying. Social media platforms have become significant mediums for individuals to exercise their freedom of expression, sharing ideas and information with a wide audience. However, this freedom must be balanced with the right to privacy, ensuring that individuals are protected from unwarranted intrusions into their personal lives or reputational harm.

In the context of cyberbullying, these rights are particularly relevant. Cyberbullying can involve the use of social media and other online platforms to harass, intimidate, or harm

[79] Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/RES/217(III) (Dec. 10, 1948), art.12.
[80] International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171, art. 19.
[81] International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171, art. 17.

individuals. While freedom of expression allows for open discourse and debate, it does not justify behavior that violates an individual's privacy or subjects them to attacks on their honor and reputation. Therefore, it is important for laws and policies to strike a balance between protecting freedom of expression and ensuring the right to privacy. This includes establishing measures to prevent and address cyberbullying while upholding these fundamental rights for all individuals, both online and offline.

III. European Convention on Human Rights (ECHR)\

European Convention on Human Rights (ECHR) highlight two fundamental rights: the right to freedom of expression (Article 10)[82] and the right to privacy (Article 8)[83].

Article 10 guarantees individuals the right to express their opinions and share information freely, without interference from the government or other public authorities. This right extends to various forms of communication, including verbal, written, artistic, and digital expressions. However, this right is not absolute and can be subject to limitations, such as those necessary to protect the rights and reputations of others or national security.

Article 8 protects individuals' right to privacy, encompassing their personal and family life, their home, and their communications. This right establishes a zone of privacy that should be free from arbitrary interference by the state or other individuals. Like the right to freedom of expression, the right to privacy is not absolute and can be limited in certain circumstances, such as for the protection of national security, public safety, or the rights and freedoms of others.

These rights are essential in the context of social media and cyberbullying, as they provide a framework for understanding the balance between individuals' freedom to express themselves online and their right to privacy and protection from harm. Balancing these rights is crucial in addressing issues such as cyberbullying, where harmful or offensive content may infringe on individuals' rights to privacy and dignity, while also considering the importance of freedom of expression in the online sphere.

IV. American Convention on Human Rights (Pact of San José, Costa Rica)

The American Convention on Human Rights, also known as the Pact of San José, Costa Rica, includes provisions related to both freedom of expression and the right to privacy.

[82] European Convention on Human Rights art. 10, Nov. 4, 1950, 213 U.N.T.S. 221.
[83] European Convention on Human Rights art. 8, Nov. 4, 1950, 213 U.N.T.S. 221.

Freedom of Expression (Article 13)[84]: This right guarantee individual the freedom to express their thoughts and opinions, and to seek, receive, and impart information and ideas through various mediums such as speech, writing, or artistic expression. This right is not limited by geographical boundaries and can be exercised in different forms.

Right to Privacy (Article 11)[85]: This right protects individuals' honor, dignity, and privacy. It ensures that individuals are not subjected to arbitrary or abusive interference with their private lives, families, homes, or correspondence. It also prohibits unlawful attacks on a person's honor or reputation.

These provisions, while fundamental, do not provide explicit definitions related to social media or cyberbullying. However, they set the framework for understanding the importance of balancing freedom of expression with the protection of individual privacy and dignity, which are particularly relevant in the context of social media and cyberbullying.

Legal Rights and Social Media

In India, the legal framework governing freedom of expression and privacy on social media is primarily rooted in the Constitution, supplemented by specific statutes and evolving case law. Article 19(1)(a) of the Indian Constitution guarantees the fundamental right to freedom of speech and expression, which extends to the digital and online domains, including social media. However, this right is not absolute and comes with reasonable restrictions under Article 19(2), which allows the state to impose limitations on grounds of sovereignty and integrity of India, security of the state, friendly relations with foreign states, public order, decency, or morality, or in relation to contempt of court, defamation, or incitement to an offence.

Privacy, on the other hand, is protected under Article 21 of the Constitution, which guarantees the right to life and personal liberty. The landmark Supreme Court decision in Justice K.S. Puttaswamy (Retd.) vs Union of India (2017) recognized privacy as an intrinsic part of the right to life and personal liberty. This ruling has significant implications for the regulation of social media, as it mandates the protection of personal data and privacy.

Further, the Information Technology (IT) Act, 2000, and the rules framed under it, particularly the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, provide a legal framework for data protection and combat cybercrimes, impacting how personal information is handled on social

[84] American Convention on Human Rights, Pact of San José, Costa Rica, art. 13, Nov. 22, 1969, 1144 U.N.T.S.123.
[85] American Convention on Human Rights, Pact of San José, Costa Rica, art. 11, Nov. 22, 1969, 1144 U.N.T.S.123.

media platforms. The Digital Personal Data Protection Bill, an amendment to the IT Rules, 2021, represents a significant step towards safeguarding freedom of expression and fundamental speech rights on social media platforms. The amendment, introduced in October 2022, mandates that platforms respect users' free speech rights and establishes three Grievance Appellate Committees to address content complaints. These committees are expected to be integrated into the broader Digital India Act. Additionally, the Act will address online safety issues such as AI, Deepfakes, cybercrime, competition among internet platforms, and data protection. It includes provisions for a new adjudicatory mechanism for online criminal and civil offenses and revisits the concept of 'safe harbor', which shields social media platforms from liability for user-generated content.

The Digital Personal Data Protection Bill focuses on regulating the processing of digital personal data, both within and outside India, if it affects individuals in India. It requires data fiduciaries to process personal data lawfully, maintain its accuracy, ensure data security, and delete data once its purpose is fulfilled. The Bill also grants individuals rights such as information access, correction, erasure, and grievance redressal, with provisions for government agency exemptions based on specified grounds. The establishment of the Data Protection Board of India is proposed to adjudicate non-compliance with the Bill's provisions.

Despite these protections, the dynamic landscape of social media poses continuous challenges, such as the balancing act between curbing fake news and protecting free expression or managing privacy in an age where digital footprints are vast and persistent. The legal responses are continually evolving, as seen with amendments to IT laws and regulations that attempt to address these complex issues. Thus, while users enjoy a broad range of freedoms online, these are tempered by legal and regulatory mechanisms aimed at ensuring responsible use of social media.

Freedom of Expression Vs. Right To Privacy

In the digital era, the intersection of freedom of expression and the right to privacy on social media presents complex legal dilemmas, particularly when these fundamental rights come into conflict. Social media platforms enable users to share information widely and rapidly, thus facilitating the exercise of freedom of expression. However, this very capacity can impinge on privacy, especially when personal information is disseminated without consent. The conflict often arises in scenarios such as the posting of private photographs without permission, the sharing of personal data for doxxing, or the use of social media to spread false information that can harm an individual’s private life or public reputation.

In India, Article 19(1)(a) of the Constitution guarantees freedom of expression, but Article 19(2) allows the state to impose restrictions on this right in the interest of sovereignty and integrity of the state, security, friendly relations with foreign states, public order, decency or morality, or in relation to contempt of court, defamation, or incitement to an offense. The balance between the Right to Privacy and the Right to Freedom of Speech is a fundamental concern. Even when one person's freedom to express ideas interferes with another's Right to Privacy, a democratic society values and upholds both rights.

The freedom to express oneself is compromised when private aspects of life are exposed to potential intrusion. Concerns arise about surveillance and analysis of thoughts, words, and interactions. Restrictions on accessing internet content hinder individuals' ability to freely transmit and receive information. Exclusion from social spheres can occur when one's online identity is revealed or when internet or phone services limit expression and information rights, exacerbating social disparities.

Violations of privacy restrict free expression, leading individuals to filter their messages and reducing their desire to join and interact. This infringement on privacy also impacts the right to freedom of association and assembly. Government monitoring of communications exposes private relationships and exchanges, affecting individuals' ability to freely express ideas and communicate with others. Surveillance can also limit the ability to organize, as online activities and location data can reveal interests and group memberships, and scanning technologies can identify individuals in physical spaces. Certain genders, such as women, are particularly vulnerable to violations of their rights to free expression, privacy, and information..

Legally, this intersection is challenging as both rights are protected under international human rights law and most national constitutions, but neither right is absolute. Courts often need to balance these rights by considering the context and potential harms. For instance, in scenarios where public interest is served by the dissemination of certain information, such as exposing corruption, freedom of expression may be prioritized. Conversely, in cases involving revenge porn or unwarranted intrusion into one's personal life, privacy rights are likely to be given precedence. This balancing act is further complicated by varying national laws and the global nature of the internet, requiring a nuanced understanding of legal principles and the specifics of each case. The resolution of such conflicts must, therefore, navigate the delicate line between upholding the public interest and protecting individual privacy, ensuring that neither right is unduly compromised.

Conflicting Rights: Analysis of Situations Where Rights Conflict on Social Media

The Right to Privacy and Freedom of Expression are often intertwined, but they can conflict in certain situations. For example, privacy claims might be used to prevent the dissemination of information about individuals, limiting reporting on matters of public interest or deliberately misleading others. However, unwarranted revelation of private information can severely impinge on the Right to Privacy, especially for individuals in vulnerable situations.To create a transparent framework for protecting both freedom of expression and privacy rights, particularly online, it's important to consider relevant provisions of international agreements like the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), as well as regional agreements such as the European Convention on Human Rights and the EU Charter of Fundamental Rights and Freedom.

The Internet is a global resource that should be managed in the public interest. While digital technologies have enhanced freedom of expression and access to information, they also pose challenges to protecting individuals' right to privacy and personal data. The release of enormous amounts of data for societal benefits raises serious risks to individuals' privacy rights and personal data.Conflicts between the right to freedom of expression and the right to privacy often emerge prominently in cases of cyberbullying on social media. Here's an analysis of how these rights may conflict and intersect in such scenarios:

I. Freedom of Expression vs. Protection from Harm

The tension between freedom of expression and protection from harm is a complex and nuanced issue, particularly in the context of cyberbullying. On one hand, individuals have the right to express their opinions and thoughts freely, as guaranteed by various national and international laws. This includes the right to express controversial or unpopular opinions, which is essential for a vibrant and diverse society where different ideas can be debated and challenged.

However, this right is not absolute and must be balanced with the need to protect individuals from harm, including emotional and psychological harm caused by cyberbullying. Victims of cyberbullying often experience severe emotional distress, anxiety, depression, and even suicidal thoughts as a result of the abusive behavior they face online.

In cases of cyberbullying, the line between free speech and harmful behavior can be blurred. While some may argue that cyberbullying is simply an exercise of free speech, victims see it as a form of harassment that infringes on their right to safety and well-being. This highlights the importance of considering the impact of one's speech on others and the

responsibility that comes with exercising the right to free expression.

Legally, many jurisdictions have laws that address cyberbullying and online harassment, recognizing that the right to free speech does not include the right to harm others. These laws aim to strike a balance between protecting individuals from harm and preserving the right to free expression, often by prohibiting speech that constitutes harassment, threats, or incitement to violence.

II. Public Interest vs. Personal Safety

The clash between public interest and personal safety is a challenging aspect of cyberbullying, particularly concerning the thin line between exposing negative behaviors and engaging in harmful online conduct. On one side, the public interest argument asserts that revealing certain behaviors or attitudes, even if they are negative, can serve a greater good by exposing wrongdoing, promoting accountability, or sparking public debate. This argument often comes into play in cases of whistleblowing, where individuals disclose information to expose corruption, misconduct, or other unethical behavior. However, this argument can sometimes be misused or distorted to justify acts that actually constitute cyberbullying. Cyberbullies may claim they are acting in the public interest by exposing supposed wrongdoing or criticizing certain behaviors, when in reality, their actions are aimed at harassing, intimidating, or harming others. This misuse of the public interest argument can undermine the genuine efforts of whistleblowers and detract from legitimate public discourse.

On the other side of the spectrum, personal safety and mental well-being are paramount concerns that necessitate restrictions on speech that directly threatens or harasses individuals. Cyberbullying can have severe consequences on victims, leading to emotional distress, anxiety, depression, and in extreme cases, even suicide. In such instances, protecting individuals from harm takes precedence over any arguments related to public interest or free speech.

Balancing these conflicting interests requires a careful consideration of the context and impact of the speech in question. While there is a need to protect free speech and the public's right to know, this should not come at the expense of individuals' safety and well-being. Legislation and policies addressing cyberbullying should take into account these complexities, ensuring that they strike an appropriate balance between public interest and personal safety. This may involve implementing measures to prevent and address cyberbullying while also safeguarding whistleblowers and legitimate forms of public discourse.

III. Anonymity and Privacy

The anonymity afforded by social media platforms can indeed be a double-edged sword. On one hand, it allows users to express their opinions and engage in discussions without revealing their true identities, which can be empowering, especially in contexts where expressing certain views might lead to backlash or discrimination. However, this anonymity can also enable harmful behaviors such as cyberbullying, harassment, and the spread of misinformation. When individuals use this anonymity to target others with malicious intent, it can infringe upon the targeted individuals' right to privacy and a life free from harassment and fear. This tension between the right to anonymity and the right to protection from harm has prompted calls for social media platforms to breach users' anonymity in certain circumstances, such as when there is evidence of harassment or other forms of abuse. Proponents argue that this is necessary to protect individuals from harm and to hold perpetrators accountable for their actions.

IV. Platform Responsibility

The issue of platform responsibility in balancing freedom of expression with the need to combat bullying and harassment is a critical and complex one. Social media platforms are often considered to be public forums where individuals can freely express their opinions and engage in discussions. However, this freedom can be abused, leading to harmful behaviors such as bullying and harassment.

Platforms are faced with the challenge of maintaining a safe and welcoming environment for users while also upholding principles of free speech. This requires them to develop and enforce policies against bullying and harassment, which may involve removing content or suspending accounts that violate these policies. At the same time, platforms must be careful not to infringe upon users' rights to freedom of expression. This raises questions about the extent of their responsibility to protect users from harmful content and behaviors. Some argue that platforms have a moral obligation to intervene and remove harmful content, as allowing it to remain can perpetuate harm and create a hostile environment for users.

Finding the right balance between protecting users from harm and upholding principles of free speech is a complex and challenging task for social media platforms. It requires them to carefully consider the impact of their policies and practices on users' rights and to continually evaluate and refine their approach in response to changing societal norms and expectations.

V. Jurisdictional Challenges

The global nature of the internet presents significant challenges in addressing cyberbullying, particularly regarding jurisdictional issues. What constitutes cyberbullying in one jurisdiction may not be recognized as such in another, leading to discrepancies in legal frameworks and enforcement measures. This complicates efforts to protect individuals from online harassment and abuse, as actions that are harmful in one country may not be considered unlawful in another.

One of the key challenges is determining which jurisdiction has the authority to regulate and prosecute cyberbullying cases that span multiple jurisdictions. This is further complicated by the fact that the internet transcends physical borders, making it difficult to apply traditional legal principles based on territorial jurisdiction.

Cross-border legal frameworks and cooperation are essential to address these challenges. International agreements and treaties can help establish common standards for defining and addressing cyberbullying, facilitating cooperation between countries to combat this issue effectively. Mutual legal assistance treaties (MLATs) and other forms of cooperation mechanisms can be used to share information, gather evidence, and extradite individuals involved in cyberbullying across borders.

Furthermore, efforts to address jurisdictional challenges in cyberbullying require collaboration between governments, law enforcement agencies, internet service providers, and other stakeholders. Establishing clear protocols and mechanisms for cross-border cooperation and information sharing can help streamline the process of addressing cyberbullying cases that involve multiple jurisdictions. In each of these points, the core issue lies in balancing the protection of individual dignity and privacy with the preservation of free expression, a task that continues to challenge legal systems, social media platforms, and society at large.

Forms and Manifestations of Victim Blaming in India

In the Legal System

The legal system in India often struggles with adequately addressing cyberbullying, especially when it intersects with victim blaming. While laws such as the Information Technology Act (2000) and specific sections of the Indian Penal Code address cybercrimes, enforcement issues persist, particularly in the context of gender. Women who experience cyberbullying and seek legal recourse frequently encounter victim blaming attitudes from law enforcement personnel, who may question their online behavior, social interactions, or even the appropriateness of their digital presence. Such responses reflect a lack of sensitivity and

understanding of cyberbullying's impact, effectively deterring many women from pursuing justice. Moreover, legal frameworks sometimes fail to keep pace with the evolving nature of cyberbullying, leaving gaps that can result in inadequate protection for victims.

In Media Portrayals

Media portrayals significantly influence public perceptions of cyberbullying and victim blaming. In India, the media often sensationalizes incidents of cyberbullying involving women, focusing on the victim's character and actions rather than the bullying behaviour. This can lead to a public narrative that implicitly or explicitly blames the victim for provoking the harassment, whether through her social media activity, the nature of the content she posts, or her public persona. Such portrayals not only skew public understanding of the nature of cyberbullying but also perpetuate a culture where women are held responsible for the aggression they endure online.

In Public Discourse and Social Media

Public discourse and social media are perhaps the most direct platforms where forms of victim blaming can be observed. The anonymity afforded by the digital space emboldens individuals to express judgments and blame towards women who experience cyberbullying. In many cases, comments on social media posts about incidents of cyberbullying focus on victim's actions such as why they shared certain content or engaged with certain individuals online rather than condemning the perpetrators. Social media thus becomes a double-edged sword: while it has the power to rally support for victims, it also serves as a platform for perpetuating victim blaming and shaming.

These discussions often reflect deeper societal norms that hold women to stricter standards of behavior and morality, especially within the digital realm. Public figures, influencers, and everyday users contribute to a discourse that may question a victim’s credibility based on her online presence and activities, reinforcing the stigma around women freely expressing themselves on digital platforms.

Cultural and Social Factors Contributing to Victim Blaming in Digital Space in India

Victim blaming in India is a significant social issue, influenced by a complex interplay of cultural, social, and legal factors. Understanding these factors can help in addressing and mitigating the phenomenon. Here are some key factors contributing to victim blaming in India:

1.Societal Norms and Cultural Conditioning-

India's diverse cultures often hold conservative views on gender roles and sexual behavior. Traditional norms can sometimes dictate strict behavior codes, especially for women, regarding

how they should dress, act, and interact in public and private spaces. When individuals, particularly women, deviate from these norms, society may blame them for any harm that befalls them, rather than holding the perpetrator accountable.

2. Patriarchal Attitudes-

The patriarchal structure of many Indian communities' places men in positions of authority and control, reinforcing gender inequality. This power imbalance can lead to a normalization of discrimination against women, including victim blaming. Women who assert autonomy be it through dressing, career choices, or lifestyle can be viewed as breaking the social order, which can lead to victim blaming when they face harassment or violence.

3. Stigmatization and Honor Concept-

In many parts of India, the concept of family or community 'honour' is closely linked to the behaviour and actions of its women members. Victims of sexual assault or harassment are often blamed for bringing dishonour to their family or community, discouraging them from reporting such incidents. This stigmatization not only perpetuates victim blaming but also prevents many victims from seeking justice.

4. Lack of Education and Awareness-

Limited educational opportunities and lack of awareness about gender equality contribute to entrenched sexist attitudes and norms. Many people in India are not exposed to concepts of gender equality or the detrimental effects of victim blaming, which perpetuates these attitudes across generations.

5. Media Portrayal –

The Indian media and entertainment industry sometimes reinforce stereotypes that contribute to victim blaming. Films and TV shows that depict women in stereotypical and subordinate roles can influence public perception and attitudes towards women, which in turn impacts how victims are perceived when they report crimes.

6. Legal and Institutional Failures -

The legal system in India can sometimes be slow and insensitive to the needs of victims, particularly in cases of sexual violence. Inadequate handling of such cases, victim shaming during legal processes, and low conviction rates can contribute to a culture of victim blaming. This is exacerbated by reports of police insensitivity or refusal to file complaints, which further discourages victims from coming forward.

7. social media and Anonymity -

The rise of digital platforms has provided new venues for victim blaming. The anonymity of the internet allows individuals to express and amplify harmful views without accountability.

Social media can spread misinformation about cases rapidly, often leading to unwarranted blame and speculation about the victim's character or actions.

Addressing these factors requires concerted efforts across multiple levels of society, including legal reforms, educational initiatives, media responsibility, and cultural change programs aimed at promoting gender equality and respect for all individuals regardless of their gender or status.

Impact on Victim's Willingness to Seek Legal Recourse

Victim blaming in the digital space has a profound impact on victims' willingness to seek legal recourse. This phenomenon occurs when victims of online harassment, cyberbullying, or digital abuse are held partially or entirely responsible for the harm inflicted upon them. The digital environment, characterized by its anonymity and lack of physical presence, exacerbates the effects of victim blaming, leading to several adverse outcomes for the individuals targeted.

Firstly, victim blaming in the digital space can significantly erode the self-esteem and confidence of the victims. When individuals are blamed for the harassment or abuse they experience online, they may internalize the criticism and begin to believe that they are at fault. This self-doubt can make them hesitant to seek legal recourse, as they may feel unworthy of protection or justice. Moreover, the fear of being judged or disbelieved by legal authorities can further deter them from pursuing legal action.

Secondly, victim blaming can lead to a sense of isolation and helplessness among victims. In the digital space, where interactions are often impersonal, victims may feel that they are facing their abusers alone. The lack of support and understanding from peers and society can exacerbate this isolation, making victims less likely to reach out for legal assistance. The feeling of helplessness is compounded when victims witness others being blamed for similar experiences, reinforcing the notion that seeking help may be futile.

Thirdly, the public nature of digital platforms can amplify the effects of victim blaming. When victims are blamed on social media or other online forums, their experiences and perceived faults are exposed to a wide audience. This public scrutiny can be humiliating and traumatic, discouraging victims from seeking legal recourse for fear of further exposure and criticism. The digital footprint of such victim blaming can also have long-lasting repercussions, affecting the victim's reputation and personal life.

Fourthly, victim blaming in the digital space can create a culture of silence and acceptance of abuse. When victims see that others are blamed for their own victimization, they may feel that speaking out or seeking legal help is pointless or even detrimental. This can lead to

underreporting of digital abuse and a lack of accountability for perpetrators, perpetuating a cycle of abuse and silence.

To counteract the impact of victim blaming on victims' willingness to seek legal recourse, several measures can be taken. Firstly, there needs to be increased awareness and education about the nature of digital abuse and the importance of not blaming the victim. This can be achieved through public campaigns, school programs, and the involvement of influencers and public figures. Secondly, legal professionals and law enforcement agencies should receive training to handle cases of digital abuse with sensitivity and without prejudice, ensuring that victims feel supported and believed. Thirdly, online platforms should implement stricter policies and reporting mechanisms to address abuse and prevent victim blaming. Lastly, support networks and counseling services should be readily available to assist victims in overcoming the trauma of abuse and victim blaming, empowering them to seek justice By fostering an environment of understanding and support, we can encourage victims of digital abuse to stand up for their rights and seek the legal recourse they deserve.

Mechanisms Of Victim Blaming: How Social Media Platforms and User Interactions Contribute to Victim Blaming

Victim blaming is a complex phenomenon where the blame for harm or misfortune is placed on the individuals who experience it, rather than on the perpetrator. This issue is especially prevalent in the context of social media, where interactions can both amplify and mitigate the mechanisms of victim blaming.

Social media often provides a veil of anonymity that can lead to deindividuation, a state where individuals lose their self-awareness and sense of accountability. In such environments, users may feel emboldened to express negative or harmful opinions without fear of repercussions. This anonymity can lead to increased instances of victim blaming, as individuals feel less compelled to adhere to social norms that would otherwise discourage such behavior.

Social media platforms are structured in a way that often creates echo chambers spaces where users are exposed primarily to opinions and information that reinforce their preexisting beliefs. This structure can exacerbate confirmation bias, where individuals interpret new information in a way that confirms what they already believe. In cases of victim blaming, echo chambers can intensify and validate users' predisposed notions about victims, particularly if these notions are biased or prejudiced.

Social media posts often provide limited information and lack the nuance and context that are typically available in face-to-face interactions or detailed reports. This brevity can lead to

misinterpretations and jumping to conclusions. Users may blame victims based on incomplete or skewed information, not taking into account the full scope of the situation or the complexities involved in the incident.

The viral nature of social media allows information and misinformation to spread rapidly. False narratives or misleading information about incidents can perpetuate harmful stereotypes and assumptions about victims. Once such misinformation gains traction, it can be challenging to correct public perception, further entrenching victim-blaming attitudes.

Social media platforms are designed to engage users through algorithms that promote content likely to generate interaction. Posts that provoke strong emotions or controversy, including those that involve victim blaming, often receive more engagement. This engagement then feeds back into the system, leading to wider dissemination of such posts and potentially normalizing victim blaming as a more acceptable viewpoint.

Counter-narratives and active moderation are essential in combating victim blaming on social media. When users and platform moderators challenge victim-blaming statements and offer alternative perspectives that empathize with the victim, it can help mitigate the spread of harmful narratives. Effective moderation policies and tools to report inappropriate content are critical in managing and reducing instances of victim blaming.

Social media platforms, through their structure and the nature of user interactions, can significantly contribute to the prevalence of victim blaming. To address this issue, it is crucial for these platforms to improve moderation, promote responsible content sharing, and encourage a culture of empathy and understanding. Users, too, must be vigilant and informed in their interactions to avoid perpetuating harmful behaviours and attitudes toward victims.

The intersection of freedom of expression, privacy, and the prevalence of cyberbullying against women on social media platforms presents a complex and challenging landscape. While freedom of expression is a fundamental right, it must be balanced with the right to privacy and protection from harm, especially in the digital age where online spaces can be breeding grounds for harassment and abuse. From a legal perspective, there is a need for clearer and more robust legislation that specifically addresses cyberbullying and online harassment, with provisions that consider the gendered nature of these offenses. Additionally, there should be mechanisms in place to hold social media platforms accountable for their role in facilitating or perpetuating cyberbullying. Technologically, social media platforms need to implement more effective measures to detect and prevent cyberbullying, such as improved reporting systems, algorithms to identify abusive behavior, and stricter enforcement of community guidelines. Furthermore, addressing victim blaming requires a shift in societal attitudes and perceptions. Education and

awareness campaigns can play a crucial role in challenging stereotypes and promoting empathy and understanding towards victims of cyberbullying.

CHAPTER VI

TOWARDS GENDER-INCLUSIVE ONLINE JUSTICE

Women belong in all places where decisions are being made. It shouldn't be that women are the exception. This includes the realms of digital platforms, where women should navigate freely without the threat of harassment or cyberbullying."-
Justice Ruth Bader Ginsburg

Redefining Digital Citizenship for Indian Women

Women in India are more prone to cyberbullying due to various societal, cultural, and gender-specific factors. One significant reason is the deeply ingrained patriarchal attitudes and gender stereotypes that prevail in Indian society. These attitudes often lead to the objectification and marginalization of women, making them more vulnerable to online harassment and abuse.

Additionally, the anonymity provided by the internet can embolden perpetrators to target women with impunity, knowing that they are less likely to face consequences for their actions. This anonymity, coupled with the lack of awareness and understanding of cyberbullying among law enforcement agencies, further exacerbates the problem. Furthermore, the rapid proliferation of social media and digital platforms in India has created new avenues for cyberbullying, with women often being targeted for expressing their opinions or asserting their rights online. This phenomenon is particularly prevalent in cases where women challenge traditional gender roles or advocate for gender equality.

Indian women's ability to engage as equal citizens in the online world is further restricted by their lack of access to safe digital spaces and significant digital literacy. Even though the government advocates for "Digital India," not everyone has benefited equally from this digital revolution. While urban women, despite having more access, encounter an invisible wall of ongoing surveillance, criticism, and retribution whenever they use their digital voice to challenge injustice, many rural women are still shut out of digital education and awareness. In its broadest definition, digital citizenship calls for more than just having internet connection; it also calls for having the confidence to exist without being erased, the freedom to participate without fear, and the opportunity to seek remedy without opposition. In order to do this, there must be a structural commitment to tearing down patriarchal digital cultures and integrating gender justice into digital

governance itself.

Furthermore, an approach to digital justice that is gender inclusive must acknowledge that online environments are not neutral; rather, they are influenced by the same power structures that control offline society. Caste, religion, sexual orientation, and occupation all have a role in how women experience social media. For example, misogynistic and racist cyberattacks targeting gay voices, Dalit activists, and female journalists are multifaceted. Therefore, addressing these intersectional realities is also a part of reimagining digital citizenship for Indian women. It calls for a feminist rethinking of cyberspace, one in which participation does not come at the expense of safety and dignity, and where access is not merely technical but transformative. In the end, achieving justice in the digital sphere requires a paradigm shift in our understanding of online rights, power, and accountability. In addition to being required by law, creating an inclusive architecture is also morally and democratically required.

Between Identity and Invisibilisation: The Gaps in Law and Recognition

According to Indian law, a woman is defined as any female human being from birth until death. This definition is in line with the broader understanding of gender identity in Indian society. However, it is important to note that gender identity is a complex and multifaceted concept that extends beyond biological sex, and the legal definition of women in India does not encompass the full spectrum of gender identities. The pervasiveness of cyberbullying against women in India underscores the urgent need for a comprehensive legal framework that effectively addresses this issue. This study has explored various dimensions of cyberbullying, including its definition, historical context, psychological impacts, and the role of social media platforms. Through a comparative analysis of international legal systems, we have identified gaps in the current legal framework in India and proposed recommendations for improvement.

Many people who identify outside of the traditional binary have their lived experiences erased as a result of the strictness of legal classifications. Though their experiences are mostly hidden by the laws that are now in place, transgender women, non-binary people, and gender non-conforming people are especially vulnerable to cyberbullying. The inability of digital safety legislation to specifically acknowledge these identities leads to their double marginalization, first by society and then by the law. This invisibilization is structural rather than merely semantic, impacting rights recognition, protection from damage, and access to justice. Any attempt to address online abuse

remains intrinsically exclusive in the absence of inclusive terminology and regulatory frameworks that take into consideration the changing concept of gender.

Additionally, the contradiction between legal stagnation and social change highlights how urgently jurisprudential reform is needed. Although Indian courts have recently adopted progressive views on privacy and gender, these developments have not yet resulted in full legislative frameworks that address cyber damage. Because of procedural prejudices or a lack of enabling legislation, victims who do not cleanly fall into traditional gender classifications are frequently denied remedy. In order to close this gap, communities impacted by digital gender-based violence must be actively consulted in addition to legal writing. All citizens, regardless of their gender identification, must be equally protected by inclusive cyberlaw, which acknowledges identity as a dynamic, context-driven concept. Enumeration is not enough for true legal recognition; it also involves guaranteeing equality, protection, and dignity in the face of harm.

Gendered Harm in the Age of Algorithms

Cyberbullying is a complex phenomenon that requires a nuanced understanding of its various forms and manifestations. It is not merely an extension of traditional bullying, but a distinct form of aggression facilitated by digital technologies. Women are disproportionately targeted by cyberbullies, highlighting the intersectionality of gender and technology in shaping experiences of victimization. The psychological impact of cyberbullying on women can be severe, leading to anxiety, depression, and even suicidal ideation. It is therefore imperative to address cyberbullying not only from a legal perspective but also from a mental health standpoint. Providing victims with adequate support and resources is crucial in mitigating the negative effects of cyberbullying.

Cyberbullying adds another level of silent suffering for women in India, where mental health services are still underdeveloped and often stigmatized. Many victims are prevented from receiving prompt counseling or mental health assistance because of institutional indifference, social anxiety, or financial limitations. The lack of prompt legal remedies and the investigation's sluggish pace exacerbate the emotional suffering. Women are frequently forced to drop accusations about morphing, doxing, or revenge pornography because of pressure from family members or threats from offenders. A deeper, systemic failure is revealed by this pattern of injury, where the victim is left to bear the burden of protection while the design of digital spaces continues to be unfriendly and unaccountable. Instead of only addressing cyberbullying as a digital crime,

acknowledging it as a public health issue can help frame more comprehensive responses based on trauma-informed legal aid, victim care, and therapeutic recovery paths.

Furthermore, it's common to ignore how algorithms shape digital abuse. Social media platforms frequently spread unpleasant or contentious content because they are fuelled by engagement metrics and content virality. Pre-existing social inequalities are sometimes reinforced by algorithmic prejudice, which increases the visibility of women, particularly those from marginalized communities, making them more susceptible to organized attacks and online mobs. Predictive systems that profit on outrage curate, promote, and monetize abuse, which is not necessarily random. Because these technology intermediaries are invisible in public debate, platform owners can avoid accountability while still making money off of clicks and shares brought about by offensive content. This presents a significant obstacle for Indian legislators and regulators: the requirement to control not only the users but also the platform design that permits and intensifies gendered harm. To guarantee that digital spaces do not continue to be coded extensions of offline patriarchy, a future-ready legislative framework must incorporate algorithmic accountability, human rights audits for platform design, and required openness in content moderation systems.

Complicity by Design: Platform Responsibility and Social Legitimacy

Social media platforms play a significant role in perpetuating cyberbullying through their design and algorithms. They often fail to effectively regulate harmful content, leading to the proliferation of abusive behaviour online. It is essential for social media companies to take responsibility for their platforms' impact on society and implement stricter regulations to curb cyberbullying. The balancing act between protecting user rights and complying with regulatory requirements is an ongoing challenge for social media platforms. This balance requires not only adherence to the law but also a strong commitment to ethical practices and respect for fundamental human rights. Achieving this balance is critical not only for legal compliance but also for maintaining user trust and the social legitimacy of these platforms.

The opaqueness of automated decision-making and content filtering procedures further muddies the waters. Under the pretense of impartiality, social media corporations use automated filters and machine-learning tools that frequently miss subtle kinds of gender-based violence, such dog-whistling, coded hate, or persistent harassment through meme culture and subtweets. On the

other hand, legitimate content that supports minority rights or feminist causes is occasionally mistakenly reported or shadow-banned. This exposes a more serious ethical failing: the platforms actively curate what is heard, seen, and silenced rather than acting as passive hosts. User confidence is further damaged by the opaqueness of the abuse report handling process, delayed takedowns, and uneven application of community norms. Such systematic platform failures increase women's vulnerability and perpetuate digital exclusion in India, where sociopolitical hurdles to expression are already present.

As a result, platform responsibility is a constitutional as well as technological issue. Platforms must be held to a higher standard of public accountability in democracies like India, where the right to life and dignity, as well as freedom of speech, are essential rights. Although due diligence standards are imposed by the existing Indian cyber law intermediary rules, enforcement is still lax and dispersed. Affirmative duties, such releasing transparency reports, localizing grievance redressal procedures, and guaranteeing significant human oversight in content moderation, must be placed on tech companies immediately. Additionally, regulatory frameworks must adopt a collaborative structure incorporating academic institutions, civic society, and advocates for digital rights in place of punitive measures. The legislation can transform platforms from commercial arbiters to constitutional collaborators in promoting gender equity online by redefining them as public-influence actors, more like digital town squares than private businesses.

Fragmented Laws, Fragmented Justice: The Case for Legal Consolidation

The legal framework governing cyberbullying in India is fragmented and lacks coherence. There is a need for comprehensive legislation that specifically addresses cyberbullying and provides clear guidelines for enforcement. The judiciary also plays a crucial role in interpreting and applying the law in cases of cyberbullying, ensuring that victims receive the justice they deserve.

The comparative analysis of cyberbullying laws across the United Kingdom, the United States, India, Canada, and Australia reveals diverse approaches shaped by cultural, legal, and technological contexts. In the UK, cyberbullying is addressed within broader communication and harassment laws, with a focus on criminal behaviors and educational policies. The US lacks federal legislation, leading to a patchwork of state laws, with examples like New York's proactive Dignity for All Students Act. India incorporates cyberbullying under the Information Technology Act, with

specific criminal provisions, influenced by the striking down of Section 66A. Canada uses criminal law and provincial policies, mandating anti-cyberbullying measures in schools. Australia has both national and state laws, with the Office of the eSafety Commissioner playing a key role. These varied approaches demonstrate the complexity of combating cyberbullying and highlight the need for multifaceted strategies.

The Indian Penal Code, 1860, the Information Technology Act, 2000, and other judicial guidelines contain a variety of provisions that make up the country's existing legal toolset, but none of them specifically identify or classify cyberbullying as a separate crime. Due to this legal ambiguity, enforcement authorities frequently reject complaints outright, create procedural obstacles, and interpret the law inconsistently. For example, whereas stalking is covered by Section 354D IPC and insult to a woman's modesty is covered by Section 509, neither law is designed to address persistent online harassment on many platforms. Similarly, even though it was hailed as a win for free speech, the deletion of Section 66A of the IT Act left a statutory void that no strong substitute could fill. Victims are left traversing a labyrinth of underutilized or misinterpreted rules in the absence of a central statute that acknowledges and classifies digital harassment, which includes doxing, trolling, impersonation, and the dissemination of deepfakes. One important piece of legislation that could help close this legal gap is a consolidated Cyber Harassment and Protection Act that provides structured remedies and codifies gender-specific safeguards.

Furthermore, without institutional preparedness, merely passing legislation is insufficient. Due to a lack of specialized training in digital crimes, police departments, cyber units, public prosecutors, and judges frequently show indifference, postpone, or misclassify major offenses. This disparity also has a constitutional component: the right to digital safety and dignity must also be viewed as part of the right to life under Article 21, especially for women whose social involvement is increasingly mediated online. Therefore, systemic investment in cybercrime infrastructure, standardized procedural norms, and victim-sensitive policies grounded on constitutional morality must all go hand in hand with legal change. Static rules and fragmented enforcement are no longer sufficient in a culture where gendered violence changes in tandem with technology. The only way to fully realize the promise of justice for victims of cybercrime, particularly women, is through institutional and statutory consolidation.

Rights in Collision: Expression, Privacy, and Protection

The confluence of freedom of expression, privacy concerns, and the prevalence of cyberbullying against women on social media platforms creates a complex and challenging environment. While freedom of expression is a fundamental right, it must be balanced with the right to privacy and protection from harm, particularly in the digital era where online platforms can serve as breeding grounds for harassment and abuse. Legislation needs to be clearer and more robust, specifically addressing cyberbullying and online harassment, taking into account the gendered nature of these offenses. Additionally, mechanisms should be established to hold social media platforms accountable for their role in enabling or perpetuating cyberbullying. Technological solutions are also crucial. Social media platforms should implement more effective measures to detect and prevent cyberbullying, including enhanced reporting systems, algorithms to identify abusive behavior, and stricter enforcement of community guidelines. Furthermore, addressing victim blaming requires a shift in societal attitudes. Education and awareness campaigns can play a pivotal role in challenging stereotypes and fostering empathy and understanding toward victims of cyberbullying.

In India, where the freedom of speech guaranteed by Article 19(1)(a) of the constitution is subject to reasonable limits under Article 19(2) in the interest of public order, decency, and morality, this conflict between rights is especially important. Women's cyberbullying frequently resides on the gray area of these restrictions, protected by abused claims of free speech while also infringing on the privacy and dignity of others. Although courts have traditionally been careful when negotiating this terrain, doctrinal clarity is desperately needed as digital interactions take over as the main means of public participation. Online anonymity can be used as a weapon against vulnerable users, particularly women, who are subjected to stalking, doxing, or morphing without any real legal protection. However, it can also be used to defend dissent. The State is required to provide safe and non-hostile digital environments, especially for marginalized genders, in light of the recognition of privacy as a basic right, which was upheld in Justice K.S. Puttaswamy v. Union of India (2017).

A significant change in platform ethics is also necessary to achieve a long-term equilibrium between these rights. Social media companies cannot claim "neutrality" when their content standards and algorithmic frameworks subject women to targeted harassment at disproportionate rates. Instead of being optional corporate goodness, transparency reports, ethical auditing of

algorithmic bias, and human rights impact evaluations must become standard practice. Platforms should investigate victim-centered design elements like digital restraining measures, trauma-informed moderation procedures, and verified complaint follow-ups from the perspective of restorative justice. On the social level, media outlets, educational institutions, and civil society organizations need to cooperate in redefining public discourse so that women's voices are not punished for being visible and that speech is never an excuse for violence. The foundation for creating a digital public sphere that is truly inclusive and equitable will be a rights-based framework that values gender sensitivity, balance, and accountability.

Closing the Loop: Collective Resolve for Safer Platforms

To effectively address and mitigate the persistent and evolving challenge of cyberbullying, the following recommendations are proposed as potential legislative, institutional, and policy-based solutions.

- To Amend existing laws, such as the Information Technology Act 2000 and the Indian Penal Code, to explicitly include definitions and penalties for various forms of cyberbullying.
- To Create graded penalties for different types of cyberbullying, based on the severity of the act and the harm caused, to act as a deterrent.
- To Establish a legal provision for victims to request and obtain protective orders against cyberbullies, requiring them to cease contact with the victim.
- To Mandate cybersecurity awareness programs that educate about the legal consequences of cyberbullying in schools, colleges, and through public campaigns.
- To Develop specialized cells within the law enforcement for quick and effective handling of cyberbullying incidents with trained personnel in cyber laws.
- To Strengthen regulations related to the anonymity and privacy of individuals online, making it legally binding for social media platforms to protect user data and cooperate with law enforcement.
- To Implement laws that require educational institutions and internet service providers to have protocols in place for mandatory reporting of cyberbullying incidents.
- To Establish legal requirements for the provision of support services to victims of cyberbullying, including psychological support and legal aid.

- To Strengthen intermediary liability clauses to hold platforms accountable for failure to respond appropriately and timely to incidents of cyberbullying reported on their platforms.
- To Introduce legal provisions for rehabilitation programs for offenders, focusing on education and community service, especially for juvenile cyberbullies.

Towards a Digital Constitutional Morality

Moreover, the role of education and awareness campaigns is emphasized as vital in shifting cultural perceptions and behaviours associated with cyberbullying. These initiatives should promote an online culture that values respect and inclusiveness, particularly highlighting the damaging consequences of cyberbullying on individuals especially women. By enhancing digital literacy and advocating for ethical online interactions, we can forge a safer digital environment that discourages abusive behaviours and fosters a supportive community ethos.

In its conclusion, the book reiterates that although the challenge of curbing cyberbullying on social media is daunting, it is indeed feasible with a coordinated approach that includes legal actions, corporate responsibility, and enhanced public awareness. The continuous dialogue among tech companies, policymakers, legal experts, and civil society is essential in evolving strategies that effectively mitigate cyberbullying. This comprehensive and sustained collective effort is crucial for ensuring that women, along with all users, can navigate social media platforms without fear of harassment or abuse, thereby making the digital world a safer and more inclusive space for everyone.