THE JUDICIARY’S TRYST WITH ONLINE GENDER-BASED VIOLENCE

An Empirical Analysis of Indian Cases and Prevalent Judicial Attitudes

November 2023
This report is part of IT for Change’s projects, ‘Recognize, Resist, Remedy: Addressing Gender-Based Hate Speech in the Online Public Sphere,’ and ‘BUILD,’ supported by the International Development Research Centre (IDRC), Canada, and the Ford Foundation, respectively.

Acknowledgments

The authors would like to thank Arti Raghavan for her valuable insights, significant support, and legal guidance. We also want to acknowledge the work of Vaishnavi Prasad, Smriti Rao, Ananya Upadhyay, Revati Pillai, Lian Joseph, and Maria Jawed—interns who worked on the classification and analysis of cases—without whom the study would not have been possible.

Conceptualization: Anita Gurumurthy, Nandini Chami, Malavika Rajkumar and Shreeja Sen

Copy editing: Sneha Bhagwat

Proofreading: Intifada P. Basheer

This report is licensed under Creative Commons License Attribution-ShareAlike 4.0 International (CC BY-SA 4.0).
## Contents

**Abbreviations** ........................................................................................................................................... 1

**Chapter I: Introduction** .......................................................................................................................... 2

1.1 Objective of the study ............................................................................................................................ 4

**Chapter II: Methodology** ...................................................................................................................... 7

2.1 Scope of the research ............................................................................................................................ 7

2.2 Sample selection .................................................................................................................................. 8

2.3 Thematic classification of cases and confirming the reliability of grouping ........................................ 12

2.4 Sub-thematic categorization and analysis of cases ............................................................................. 14

2.5 Limitations of the study ...................................................................................................................... 15

**Chapter III: Findings** ........................................................................................................................... 20

3.1 Finding 1: Gaps in the Indian judiciary’s understanding of the online public sphere based on its adjudication of OGBV ............................................................................................................................. 20

3.2 Finding 2: Courts have increasingly begun to recognize and implement the right to privacy in OGBV cases, following the *Puttaswamy* ruling of the Supreme Court in 2017 ................................................................. 29

3.3 Finding 3: OGBV cases illustrate concerns of digital evidence and lack of understanding while issuing specific bail orders, reflecting challenges arising due to emerging technology within the criminal justice system .......................................................................................................................... 37

3.4 Finding 4: Courts are attempting to hold platforms accountable in OGBV cases, leading to emerging jurisprudence on social media governance in India ......................................................................................... 54

3.5 Finding 5: Courtrooms continue to be sexist and patriarchal spaces for survivors of OGBV cases, thereby perpetuating common judicial stereotypes and impacting access to justice ................................................................. 63

3.6 Finding 6: Courts fail to recognize power differentials among perpetrators and survivors in OGBV cases ........................................................................................................................................ 69

**Chapter IV: Conclusion and Recommendations** ................................................................................ 77

4.1 Courts must recognize the importance of the online public sphere and give equal importance to online gendered offenses ................................................................................................................................... 78

4.2 NCIID requires specific and dedicated steps for redressal, including from courts as well as the legislative process .............................................................................................................................................. 79

4.3 Courts must move beyond misplaced notions in OGBV cases and deliberate on reforming institutional processes and procedures .................................................................................................................. 80

4.4 Courts must not let procedural hurdles, including digital evidence certification, impede proper justice delivery and must contextualize bail orders for the online space ............................................................................... 80

4.5 Courts must identify challenges in holding digital platforms accountable for profitable viral content 81

4.6 The criminal justice system must undertake ecosystem-level changes in sensitization and inclusive policies ............................................................................................................................................. 81

**Endnotes** .................................................................................................................................................... 82
### Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>CDR</td>
<td>Call Detail Records</td>
</tr>
<tr>
<td>CoE</td>
<td>Council of Europe</td>
</tr>
<tr>
<td>CrPC</td>
<td>Code of Criminal Procedure, 1973</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technologies</td>
</tr>
<tr>
<td>IEA</td>
<td>Indian Evidence Act, 1872</td>
</tr>
<tr>
<td>IPC</td>
<td>Indian Penal Code, 1860</td>
</tr>
<tr>
<td>IT Act</td>
<td>Information Technology Act, 2000</td>
</tr>
<tr>
<td>IT Rules</td>
<td>Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021</td>
</tr>
<tr>
<td>NCIID</td>
<td>Non-Consensual Intimate Image Distribution</td>
</tr>
<tr>
<td>OGBV</td>
<td>Online Gender-Based Violence</td>
</tr>
<tr>
<td>PIL</td>
<td>Public Interest Litigation</td>
</tr>
<tr>
<td>POCSO</td>
<td>Protection of Children from Sexual Offences Act, 2012</td>
</tr>
<tr>
<td>PW</td>
<td>Prosecution Witness</td>
</tr>
<tr>
<td>TFGBV</td>
<td>Technology-Facilitated Gender-Based Violence</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
</tbody>
</table>
Chapter I: Introduction

The legacy of the Indian criminal justice system is a unique mix of British-era legislation, post-Independence contexts, and legal interpretations added by the judiciary. Over the years, there have been significant additions and reviews to the system—to substantive as well as procedural criminal laws—including amendments to the Code of Criminal Procedure, 1973 (CrPC), and the institution of several criminal law reform committees. Key elements have been added to the Constitution in the form of fundamental rights like the right to equality, life, and personal liberty, as well as right against self-incrimination. The contours of many of these laws and rights have been added by courts, including the right to a free, fair, and speedy trial. Courts, thus, use their orders and judgments to communicate the law, making the language of their verdicts significant.

The Indian Penal Code, 1860 (IPC), has several dedicated provisions to punish specific offenses committed on grounds of gender. Gendered violence, especially in the public sphere, is understood as a form of control over women and other marginalized groups, and is often normalized. The introduction of the internet and online spaces has paved the way for newer forms of engagement and a new public sphere, which has also meant that the structures of the offline world have shifted to the online space. These new forms of violence in the online space have come to be known either as technology-facilitated gender-based violence (TFGBV) or online gender-based violence (OGBV).

Research suggests that women are both disproportionately targeted and suffer serious consequences as a result of online violence.

Online or technology-facilitated gender-based violence are forms of gender injustice and discrimination that take place in online spaces and result in (or are likely to result in) physical, sexual, psychological, and economic harm or suffering. It may also include the exploitation of the individual’s circumstance, characteristics, or vulnerabilities. This type of online violence can include stalking, gender trolling, harassment, cyberbullying, and unsolicited pornography, among other actions. A brief by UN Women on online and information and communication technologies (ICT)-facilitated violence against women and girls during Covid-19 defines online violence as extending to “any act of gender-based violence against women that is committed, assisted or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately.”

Since March 2020, the Covid-19 pandemic has led to an exponential increase in violence against women. Owing to the pandemic and the consequent quarantining and self-isolation measures, internet usage increased between 50% to 70%. In India, by December 2021, the internet user base increased by almost 37%, compared to 2019. Women and girls started using the internet with greater
frequency during the pandemic, despite the digital gender divide. Consequently, there has also been an exponential surge in instances of gendered violence and harassment of women in online spaces.

Online forms of violence against women and girls impact psychological, social, and reproductive health. They are also often associated with offline physical and sexual violence for victims/survivors. The persistence of OGBV has a chilling effect on women’s participation in online spaces. Research suggests that women tend to self-censor and restrict their online access upon facing online violence. This is, in large part, due to sociocultural factors—including family reputation, scope of revictimization or further victimization at the police station as well as not believing their complaint or minimizing its seriousness—that also act as barriers against victims/survivors approaching legal recourses. Despite the rise in OGBV, it is often trivialized due to authorities taking poor punitive action, which is further exacerbated by victim blaming. Indian courts have often failed to mention the terms ‘online gender-based violence’, ‘technology facilitated gender-based violence’, or other similar terms while deciding cases. The bulk of the literature available on OGBV in India is in the form of studies conducted by civil society and policy actors.

In December 2021, India’s Ministry of Home Affairs set up a Committee for Reforms in Criminal Laws. While this committee is trying to factor in the evolving language of hate speech, especially in the digital space, it has overlooked one critical aspect of reforming legacy laws, as Bhavna Jha writes for Bot Populi: “Any effort to reform India’s Criminal Laws will fail without a feminist review of laws that are blind to the reality of spatial fluidity in a post-digital society.”

The existing patchwork of laws is inadequate to sufficiently address the complexities of the lived realities of violence in the digital sphere. The current legal provision on hate speech—Section 153A of the IPC—does not mention gender expressly as one of its protected categories. In the absence of a specific legal provision to address gender trolling, the police resort to deploying Sections of the IPC pertaining to criminal defamation (Section 499 and 500) or criminal intimidation (Section 506). Since these provisions do not encapsulate the harm caused by OGBV, the police may find it difficult to establish a case that stands in court, directly addressing online harm.

In order to make online spaces safe for women, governments must review and update legislation and policies to fully protect people from OGBV. Current laws predate important technological advances and do not adequately respond to the internet’s global and ever-evolving nature. In many cases, laws have been amended over a decade ago. For instance, the gender-focused criminal law amendments happened in 2013, and digital evidentiary requirements came into effect in 2000. For a country that is looking at an active internet user base of 900 million by 2025 (a 45% increase in five years), outdated laws can often lead to inadequate resolution of emerging issues like online harassment.
adequately address the rampant sexism and misogyny prevalent online, states must apply a human rights-based approach<sup>23</sup> to policies and practices to protect users from harm.

Numerous international human rights instruments guarantee, among other things, rights to privacy and freedom from violence and abuse. For example, Article 12 of the Universal Declaration of Human Rights recognizes a person’s right to protect themselves against privacy violations.<sup>24</sup> They also impose obligations on states to honor and protect those rights and, in some cases, to ensure that non-state actors, such as corporations, respect them as well. The United Nations (UN) Human Rights Council and the General Assembly have confirmed that, “The same rights that people have offline must also be protected online.”<sup>25</sup>

1.1 Objective of the study

The study attempts to understand judicial attitudes towards cases of OGBV by reading and analyzing our dataset of cases.<sup>26</sup> The study offers empirical evidence in the form of court orders to show that existing concerns of access to justice in the offline space are also replicated in cases of online violence.

At a time when OGBV continues to increase,<sup>27</sup> especially in India, it is crucial to understand how justice can be achieved. IT for Change’s ‘Recognize, Resist, Remedy: Addressing Gender-Based Hate Speech in the Online Public Sphere’ project<sup>28</sup> offers a platform to understand the legal and institutional frameworks that address online violence, particularly gendered hate speech. To this end, we have attempted to analyze the judiciary’s response to cases of OGBV to see how cases of online violence are remedied.

The law comes to life through individual cases. Thus, our research based on analyzing court orders—detailed in the next chapter—indicates trends in the interpretation of the law. Such a remedy-based approach helps understand how online violence is perceived in courtrooms.

This study also draws from the foundational value that laws on OGBV should be rooted in the gender-just and feminist principles of substantive equality—recognizing that individuals and groups may have special needs that must be addressed to achieve equality in outcome rather than formal equality, which assumes all people and groups should be treated exactly the same way; privacy, which includes aspects of personal autonomy, bodily integrity, and informational privacy; and dignity.<sup>29</sup> These three cornerstones are at the core of this study and the subsequent chapters.

1.1.1 Key research questions

The key questions this study attempts to answer are:

1. How are courts adjudicating cases of OGBV?
2. Do existing laws offer adequate protection against cases of OGBV? What are the legal frameworks being used while deciding these emerging offenses?

3. How do courts address cases of online violence in the context of patriarchal norms and existing gendered stereotypes?

4. What are the emerging challenges the criminal justice system faces regarding cases of OGBV?

5. How are courts holding digital platforms accountable?

In the following chapters, we have tried to answer some of these questions. Chapter 2 provides an in-depth view of the methodology for analyzing the case orders and includes the limitations of the study. Chapter 3 discusses the six key findings of the study:

1. Finding 1: Gaps in the Indian judiciary’s understanding of the online public sphere based on its adjudication of OGBV

2. Finding 2: Courts have increasingly begun to recognize and implement the right to privacy in OGBV cases, following the Puttaswamy ruling of the Supreme Court in 2017

3. Finding 3: OGBV cases illustrate concerns of digital evidence and lack of understanding while issuing specific bail orders, reflecting challenges arising due to emerging technology within the criminal justice system

4. Finding 4: Courts are attempting to hold platforms accountable in OGBV cases, leading to emerging jurisprudence on social media governance in India

5. Finding 5: Courtrooms continue to be sexist and patriarchal spaces for survivors of OGBV cases, thereby perpetuating common judicial stereotypes and impacting access to justice

6. Finding 6: Courts fail to recognize power differentials among perpetrators and survivors in OGBV cases

In Chapter 4, this study concludes with a few key observations and recommendations based on the empirical evidence noted. We explore the multiple, emergent issues of access to justice in court orders, including sexist courtrooms, lack of judicial training in feminist points of view, cisgender-focused legal provisions resulting in more cis-het women filing cases as opposed to those of gender identities or who belong to marginalized communities. We observed that while courts have started to hold platforms accountable for third-party content hosted on their platforms despite the sweeping safe harbor provisions in the Information Technology Act, 2000 (IT Act), we argue that more responsibility needs to be attributed to intermediaries by courts. We found that courts are increasingly aware, albeit in a handful of cases, of the violation of victim's/survivors' privacy rights due to OGBV. This is a positive development in the push to recognize core rights violations, instead of relying on patriarchal tropes of
modesty peppered across the text of the Indian criminal law. One of the stark observations we conclude with is the lack of recognition of gendered hate speech as a concept, which is a result of the systemic exclusion of gender as a qualifier for hate speech cases and the normalization of abuse, misogyny, and power imbalance online.
Chapter II: Methodology

2.1 Scope of the research

The objective of this study is to investigate what types of OGBV cases are filed in courts in India and understand the different types of judicial responses to these cases, including the patterns that emerge out of these cases. Given the global increase in emerging forms of TFGBV, it is imperative to glean how the Indian judicial system recognizes and deals with them. The modest scale of the research we were able to undertake through two weeks of data collection, in the form of case laws, is a humble attempt at finding qualitative insights about existing challenges to accessing justice and identifying recurring patterns.

2.1.1 Deciding on a methodology

In early 2021, the researchers attempted to decode court orders by segregating cases using an Indian Kanoon API (application programming interface) that extracted cases based on certain keywords that are commonly referenced in cases of online violence. The complete list of these keywords can be seen in Figure 1.

Figure 1. List of keywords for initial research in 2021

<table>
<thead>
<tr>
<th>1st level</th>
<th>2nd level</th>
<th>3rd level</th>
</tr>
</thead>
<tbody>
<tr>
<td>mobile phone</td>
<td>vulgar</td>
<td></td>
</tr>
<tr>
<td>facebook upload</td>
<td>husband</td>
<td>filthy</td>
</tr>
<tr>
<td>&quot;social media&quot;</td>
<td>wife</td>
<td>indecent</td>
</tr>
<tr>
<td>message</td>
<td>girl</td>
<td>&quot;outrage the modesty&quot;</td>
</tr>
<tr>
<td>posting</td>
<td>boyfriend</td>
<td>defamatory</td>
</tr>
<tr>
<td>email</td>
<td>girlfriend</td>
<td>sexism</td>
</tr>
<tr>
<td>&quot;blue film&quot;</td>
<td>sexual orientation</td>
<td>obscene</td>
</tr>
<tr>
<td>emoji</td>
<td>gender identity</td>
<td>offend</td>
</tr>
<tr>
<td>internet</td>
<td>victim</td>
<td>harassment</td>
</tr>
<tr>
<td>online</td>
<td>prosecutrix</td>
<td>insult</td>
</tr>
<tr>
<td>twitter</td>
<td>complainant</td>
<td>modesty</td>
</tr>
<tr>
<td>whatsapp</td>
<td>daughter</td>
<td>immoral</td>
</tr>
<tr>
<td>trolling</td>
<td>pornographic</td>
<td></td>
</tr>
<tr>
<td>photo</td>
<td>sexually explicit</td>
<td></td>
</tr>
<tr>
<td>nude video film</td>
<td>hate</td>
<td></td>
</tr>
<tr>
<td>camera</td>
<td>incitement to hate</td>
<td></td>
</tr>
<tr>
<td>capture of images</td>
<td>stalking</td>
<td></td>
</tr>
<tr>
<td></td>
<td>voyeurism</td>
<td></td>
</tr>
<tr>
<td></td>
<td>criminal intimidation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>grossly offensive</td>
<td></td>
</tr>
<tr>
<td></td>
<td>menacing character</td>
<td></td>
</tr>
<tr>
<td></td>
<td>identity theft</td>
<td></td>
</tr>
<tr>
<td></td>
<td>violation of privacy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cruelty</td>
<td></td>
</tr>
<tr>
<td></td>
<td>sexual favour</td>
<td></td>
</tr>
<tr>
<td></td>
<td>sexually coloured</td>
<td></td>
</tr>
<tr>
<td></td>
<td>low</td>
<td></td>
</tr>
<tr>
<td></td>
<td>humiliate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>dignity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>honour/honor</td>
<td></td>
</tr>
<tr>
<td></td>
<td>blackmail</td>
<td></td>
</tr>
</tbody>
</table>

Source: IT for Change
This yielded 26 relevant cases based on which the researchers attempted to understand certain key questions:

1. Where in the digital space did the violence take place?
2. How did the violence occur through the digital?
3. Who was targeted?
4. Why were they targeted?
5. Why did the victims/survivors approach the court?
6. What was the outcome of the case?

This approach studied only high court cases and not subordinate court cases, as it was difficult to source cases from lower courts. Additionally, the high court cases went on appeals or applications for bail. A lot of them were cases of intimate partner violence. Those that did address OGBV had not reached a decisional stage at the high court where they had been filed when the study was undertaken.

As the above method offered limited results, we proceeded with the research using the methodology discussed in the following section.

2.2 Sample selection

The first step in our research process was to identify the platform to access digital copies of public record cases. We had three options before us which included Indian Kanoon (an open-source platform), the e-Courts website (the official website maintained by the Department of Justice, Government of India), and SCC/Manupatra (paid, private online databases of cases). We faced limitations in accessing court orders from e-Courts, as it required details to search a case, including party names, case type, year and case number, which restricted any possibility of searching based on a set of chosen criteria. SCC and Manupatra also had their limitations not only because they were proprietary and paid but also because they did not feature subordinate court cases, primarily keeping a record of high court or Supreme Court cases. We chose Indian Kanoon for two reasons: first, it is a free and open-source platform, and second, it allowed us to use filter searches to identify the type of cases required for this study, i.e., those dealing with OGBV.

2.2.1 Filtering criteria

On Indian Kanoon, we relied on a four-step filtering process to narrow down OGBV cases. The sampling was purposive, which was essential to finding the type of cases required for this study. We selected cases based on the court which had given the order, a specified time period to which the search was
restricted, a set of legal provisions that would lead to the kinds of cases this study required, and finally, a few keywords to narrow the scope of the search. Each criterion is detailed below:

1. **Types of courts:** We wanted to find more subordinate court cases to trace how justice is delivered at the district level. These ‘courts of first instance’ are the ones in which most criminal and civil cases commence.

2. **Time period:** We used the time frame of cases with orders between January 2015 and November 2021, as we wanted to identify cases that came after the *Shreya Singhal* case.\(^{35}\) This case struck down Section 66A of the IT Act, relating to restrictions on online speech, as unconstitutional on grounds of violating the freedom of speech guaranteed under Article 19(1)(a) of the Constitution of India.

3. **Legal provisions:** India addresses OGBV through two main laws—the IPC and the IT Act. We referred to relevant Sections of these laws along with two prevalent, related laws for finding patterns of violence—the defamation law (Section 499, IPC) and the Indecent Representation of Women (Prohibition) Act, 1986 (some states, like Tamil Nadu,\(^ {36}\) have enacted state legislations on this). The following provisions were used from these laws to narrow down the sample size of cases.

   a. Information Technology Act, 2000: Section 66C (punishment for identity theft), Section 66D (impersonation), Section 66E (punishment for violation of privacy), Section 67 (punishment for publishing or transmitting obscene material in electronic form), Section 67A (punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form), Section 67B (punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form).

   b. Indian Penal Code, 1860: Section 354 (assault or criminal force to woman with intent to outraging her modesty), Section 354A (sexual harassment and punishment for sexual harassment), Section 354C (voyeurism), Section 354D (stalking), Section 499 (defamation), Section 292 (sale, etc., of obscene books, etc.), Section 506 (punishment for criminal intimidation), and Section 509 (word, gesture or act intended to insult the modesty of a woman).

   c. The Indecent Representation of Women (Prohibition) Act, 1986: Section 4 (prohibition of publication or sending by post of books, pamphlets, etc., containing indecent representation of women).
4. **Keywords:** We chose seven primary keywords as filters: sexual harassment, hate speech, internet, social media, defamation, threats and intimidation, and cyber violence. We wanted to define the scope of the search using these subject matters. We also wanted to see how the courts were using these terms in their orders.

We later expanded our scope to include high court cases because it was difficult to find subordinate court cases in India. This happens due to such courts not being considered 'court of records'—a court whose proceedings are enrolled for perpetual memory and testimony. As per the Indian Constitution, only the Supreme Court and high courts are deemed to be court of records. For subordinate courts, we were restricted to Delhi and Bengaluru on Indian Kanoon. Within high court cases, we were able to find scenarios of online violence through references to the fact situations within the orders. We did not restrict ourselves to a particular type of case; our data sample includes appeals, original petitions, bail orders, and anticipatory bail orders.

We extracted cases for two weeks—the last week of November 2021 and the first week of December 2021—which gave us a sample size of 93 cases that fit our parameters.

### 2.2.2 Collection of data points

After we listed the cases, we reviewed the orders to scrape the following data points:

1. **Case/order title:** The full case title
2. **Year:** The year the order was passed
3. **Court:** The court that passed the order, which could be a subordinate court or a high court of a particular state
4. **Decision/outcome:** The kind of order passed by the court, the nature of bail order passed, protection order passed, etc.
5. **Is this an appeal:** Only for high courts or Supreme Court cases to capture any associated lower court cases
6. **Law/Sections:** The laws or provisions used in the order for adjudication
7. **What is the case about:** Brief explanation of the facts of the case and the online violence element
8. **Relevant parts of the case:** The key lines or paragraphs in the order for quick reference
9. **Primary filters:** Which of the seven primary keywords mentioned earlier were used to find the case
10. **The digital medium of the offense:** The electronic platform or channel through which the offense was perpetrated. For example, platforms like WhatsApp, Facebook, Twitter/X, YouTube, etc.

11. **The method of facilitation of the offense:** The means used to enable the OGBV. For example, through videos, photos, recordings, MMS, messages, etc.

12. **Who was targeted:** Was the victim/survivor a cis-het woman, a minor, or a person from the LGBTQIA+ community

13. **Why were they targeted:** Potential reasons for the offense, wherever available in the order. This included social inequalities, like caste, or a power imbalance arising from the location of the perpetrator, like an employer, a teacher, etc.

14. **Why did they approach the court:** The reason for the plaintiff/petitioner coming to the court, including seeking punishment, compensation, regular bail, anticipatory bail, etc.

**2.2.3 Courts and types of orders**

After the data was collected, we finalized the sample data based on the courts from which the order was received (Table 1) and the types of orders extracted.

<table>
<thead>
<tr>
<th>Court</th>
<th>Number of orders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allahabad High Court</td>
<td>2</td>
</tr>
<tr>
<td>Andhra Pradesh High Court</td>
<td>2</td>
</tr>
<tr>
<td>Bengaluru District Court</td>
<td>4</td>
</tr>
<tr>
<td>Bombay High Court</td>
<td>3</td>
</tr>
<tr>
<td>Calcutta High Court</td>
<td>3</td>
</tr>
<tr>
<td>Chhattisgarh High Court</td>
<td>2</td>
</tr>
<tr>
<td>Delhi District Court</td>
<td>17</td>
</tr>
<tr>
<td>Delhi High Court</td>
<td>10</td>
</tr>
<tr>
<td>Gujarat High Court</td>
<td>1</td>
</tr>
<tr>
<td>Himachal Pradesh High Court</td>
<td>2</td>
</tr>
<tr>
<td>Jharkhand High Court</td>
<td>2</td>
</tr>
<tr>
<td>Karnataka High Court</td>
<td>4</td>
</tr>
<tr>
<td>Kerala High Court</td>
<td>10</td>
</tr>
</tbody>
</table>
The below are the types of case orders we observed:

1. Bail (Anticipatory Bail and Regular Bail),
2. Substantial Trials in District Courts,
3. High Court Cases (Appeals, Writs and Original Suits, Revision), and
4. Supreme Court Cases (PILs (Public Interest Litigations) and Appeals).

After collecting the relevant details for each case based on the 15 data points mentioned in section 2.2.2, we thematically categorized them based on the recurring patterns that emerged while analyzing them. These themes were arrived at inductively through multiple rounds of review.

2.3 Thematic classification of cases and confirming the reliability of grouping

Our initial grouping was based on six trends that emerged while collecting data. We grouped cases into these emerging themes based on certain criteria listed in Table 2.
Table 2. Thematic classification of the sample set of cases

<table>
<thead>
<tr>
<th>Emerging theme</th>
<th>Cases classified under the theme</th>
</tr>
</thead>
<tbody>
<tr>
<td>OGBV</td>
<td>Cases of hate speech, gender trolling, hateful comments against a person on social media, using social media to write hateful language, defamatory statements online, threats and intimidation to publish private images and videos online, image-based sexual abuse; any instances of hate or harm directed at women in the online public sphere/social media, including trolling, hateful words used against women, etc.</td>
</tr>
<tr>
<td>Privacy violations</td>
<td>Cases about the right to privacy; cases where the judge mentions privacy violation; and actual instances of privacy violation, like cases of voyeurism, non-consensual intimate image distribution (NCIID), etc.</td>
</tr>
<tr>
<td>Issues with the criminal justice system</td>
<td>Cases with concerns about digital evidence, burden of proof, bail, and anticipatory bail</td>
</tr>
<tr>
<td>Social media governance</td>
<td>Cases with references to social media, social media as a means to perpetrate violence on the internet, social media platform involvement, and platform regulation and accountability by courts</td>
</tr>
<tr>
<td>Sexism, patriarchy, misogyny</td>
<td>Cases involving judicial stereotyping, sexist arguments from lawyers, forms of sexism—benevolent sexism on the reputation, marital status of women, and protectionist attitude from judges</td>
</tr>
<tr>
<td>Power imbalance</td>
<td>Cases related to minors, any fiduciary relationships, occupational relationships, and absence of autonomy</td>
</tr>
</tbody>
</table>

By the end of the initial grouping stage, each case was individually appraised by four coders. Disagreements about the classification based on the themes were resolved by the coders through a consensus-building process. We also agreed that there could be an overlap in situations, where a case could fall under any of the six themes. In such situations, we ensured that if a case fit in any theme, it could be classified under it. For example, a case could be an issue directly pertaining to ‘sexism, patriarchy, misogyny’ but could also fall under ‘power imbalance’.

Based on the first round of verification of the classification, a set of sub-themes emerged under each parent theme. For the second round of verification, along with the first level of classification, the sub-theme grouping was also verified. The classification was approved if there was at least a 75% agreement (3 of the 4 coders agreed to the classification). Otherwise, it was removed from that theme and sub-theme.
2.4 Sub-thematic categorization and analysis of cases

After agreeing on the thematic split of the cases, we categorized the 94 cases under the decided themes. The sub-themes discussed below emerged from patterns within the initial themes. The sub-themes provided indicators for analyzing the cases in depth.

2.4.1 For OGBV

Under this theme, the prevalent classification became the type of violence being perpetrated, as listed below:

1. NCIID
2. Hate speech and gender trolling cases
3. Other cases (other crimes)

2.4.2 For privacy violations

For issues of privacy violations, the theme that emerged was cases that expressly mentioned or discussed a breach of this right. So, the themes were:

1. Cases that explicitly mentioned the right to privacy or recognized a violation of privacy
2. All other cases where privacy violations were not recognized but should have been due to inherent privacy violations

2.4.3 For issues with the criminal justice system

Under this theme, two types of cases emerged:

1. Digital evidence
2. Bail orders

2.4.4 For social media governance

Within this theme, we observed two types of cases:

1. Cases that recognized the role of social media
2. Cases that mentioned violence on social media

2.4.5 Regarding sexism, misogyny, and patriarchy

For this theme, we classified cases based on who made the statement in a particular case. This was done to identify the various avenues that often make courtrooms difficult spaces to navigate. As is clear from the classification below, there were cases where both judges and lawyers made statements that were rooted in stereotypes:
1. Statements by judges
2. Statements by lawyers

### 2.4.6 For power imbalance

This theme offered a view into the different types of relationships or situations through which such violence was perpetrated:

1. Minor young adult harm
2. Harms within workplaces
3. Familial relationship other than spouse
4. Ex-spousal relationships

At this stage, after multiple rounds of inductive classification, we started forming conclusions regarding our sub-theme categorizations as we deeply studied the patterns in cases within a theme. It is based on the sub-theme classification that we were able to identify indicative trends, patterns, and findings for this research study, details of which have been discussed in the following chapters.

### 2.5 Limitations of the study

A primary limitation of our study is the small sample size. We worked with a limited sample size because it is challenging to access court orders and Indian Kanoon also did not have a repository of cases across all courts. For example, we were only able to look for cases from just two subordinate courts—Delhi District Court and Bengaluru District Court. Furthermore, we did not find a reliable, open-source legal database, apart from Indian Kanoon. We also faced several limitations in terms of obtaining subordinate court cases, as they are not deemed as courts of record in Indian law. The limited number of cases we could access is also reflective of the lack of digitalization in subordinate courts, and the limited resources that these courts work with.

The second concern of our study is around defining what constitutes an online gender-based offense. This was addressed using provisions of law that focused on technology and using keywords, as discussed in section 2.2.1. This often led to situations where there were multilayered offenses with both offline and online impact. In several situations, threats to publish intimate content online coerced women to engage in further sexual activity. In effect, most cases in our study have hybrid—a mix of offline and online—offenses, making it difficult to classify cases as solely those of online violence. In many ways, this bolsters the argument that online and offline spaces are a continuum, each with specific concerns but also with significant overlaps with the other.
Furthermore, because of the variety of provisions in the Indian legal system, we were unable to find direct cases of online gendered hate speech in courtrooms. We believe this is not only due to the absence of a specific law but also due to related issues in accessing justice, including the difficulty in filing cases, delays in courtrooms, high burden of proof in such cases, etc.

We also found that most of the cases that came to courtrooms were the ones where the victims/survivors were cis-het women and did not include other gender identities or people with disabilities. While there were a few cases with provisions of The Scheduled Castes and the Scheduled Tribes (Prevention of Atrocities) Act, 1989, these did not recognize the relationship between gendered offenses and caste hierarchies. Further, we did not see any recognition of class or religion as a determining factor for the cases in the study. This limitation is also indicative of how access to justice for intersectional and marginalized groups is a concern in the judicial system. This also reflects the systemic failure of the criminal justice system in providing access to justice to minorities, including LGBTQIA+ people, people belonging to marginalized caste groups, etc. 39

Despite the small sample size, we believe that the indicative trends emerging in our study are noteworthy, especially at a time when the online world continues to develop and present newer challenges to effective law enforcement. These themes prove the existing theories of gendered issues of access to justice and the inability of the justice system to account for the particular challenges of the online public sphere.

Through the research findings in the following chapter, we hope to indicate how the judicial system deals with different issues of OGBV and trending patterns visible within the courts.
Recognizing tensions in the system

This study is the result of a review of many different judicial orders, ranging from simple bail-related cases to more fundamental questions of law in the form of writ petitions. Focusing on OGBV, these cases present myriad aspects to study, which have been discussed in brief already in the methodology section. There are emerging tensions in the cases that need to be addressed at the outset to ensure that the findings of the study can be contextualized appropriately in the Indian legal system. Given the ambit of this research, we find the following aspects pertinent to discuss before diving into the findings.

Civil and criminal remedies: What is required for OGBV?

When a subject of the state seeks judicial relief or a judicial remedy, a court of law may enforce a right, impose a penalty, or make another court order to impose its will while exercising civil law jurisdiction. Statutory civil remedies can include general statutory civil remedies, such as perpetual/mandatory/temporary injunctions, declaratory actions, specific performance, restitution, recovery of legal costs (advocate fee, court expenses, etc.), recovery of possession of liquidated, unliquidated, and statutory property or damages. Criminal remedies, on the other hand, include punishments, monetary compensations, and specific actions, for instance, seizing infringing copies and delivering them to the owner if it is an intellectual property crime.

In the Indian context, keeping in mind OGBV, the IT Act paves the way for a statutory remedy to hold perpetrators liable. However, the online violence aspect of OGBV is not highlighted because the IT Act focuses on a range of issues. Further, while looking at the IPC with regard to provisions for addressing online violence, criminal liability is not a foolproof solution and should only be used as a last resort. This is because there are several issues in criminal law remedies that need to be considered and require long-term reform. Many of the applicable offenses in the IPC do not adequately reflect the nature of some of the offending behaviors in the online environment, and the degree of harm they can cause. There are also a large number of overlapping offenses that may be confused when criminal law is applied to them. This could result in a charge sheet being made at the investigation stage or the adjudication witnessing offenses with the highest penalties. This brings the focus back to ‘punishing’ the perpetrator, or the victim–perpetrator binary, as opposed to addressing the systemic issue of online violence. Further, in criminal law, terms such as “outraging modesty”, “obscenity”, and “indecency” are very interpretative and require more clarity when contextualized with the online public sphere.

India needs more national-level responses to address OGBV with a higher focus on civil-law-based remedies that hold digital platforms and other entities liable for promoting online violence, as opposed
to criminal law sanctions. Some of the effective ways to address the problem and the virality of hate online include recognizing the role of digital platforms in facilitating violence, instituting measures to effectively moderate social media coupled with due diligence and transparency requirements, including setting clear standards for the industry and putting mechanisms in place to monitor progress. With new laws, like the Digital India Bill, coming up, focusing on online harms and holding social media platforms liable are the only ways to systematically address these issues. It is important to highlight the need for India to revisit an effective statutory civil remedy for online violence. We hope to show, over the course of the following chapters, the dichotomy of issues in the way the IPC is used as opposed to the IT Act and the lacune in effective access to justice.

**Horizontal application of fundamental rights**

An important facet of this study is the right to privacy, now a fundamental right recognized under Article 21 of the Constitution, through the nine-judge Supreme Court decision in *K.S. Puttaswamy v. Union of India*. As such, fundamental rights are enforceable against the state, i.e., the state has a duty to uphold them and is accountable to citizens for the same. Horizontal application of fundamental rights—enforcing fundamental rights against non-state actors, including other individuals or private entities—is a much-debated concept, even in India. Of course, courts have enabled some rights to be applicable even against non-state actors, in particular Articles 15(2) (prohibition of discrimination on grounds of religion, race, caste, sex or place of birth, specifically phrased in a universal manner), 17 (abolition of untouchability), and 23 (prohibition of traffic in human beings and forced labor).

This is significant to this study since we have approached OGBV based on the core principles based on equality, privacy, and dignity. The enforceability of this triumvirate is key to achieving the goals of justice for those who have suffered these newer forms of violence.

It is interesting to note that in January 2023, the Supreme Court engaged with the question of whether fundamental rights could be enforced against private individuals. In *Kaushal Kishor v. State of Uttar Pradesh*, the Supreme Court noted that it is a complex issue, one that the court, in its history, had not always favored. However, certain rights have still been available in a horizontal manner. The court, in its majority ruling, upheld the applicability of Article 21 against non-state actors as well. “[T]he State is under a duty to affirmatively protect the rights of a person under Article 21, whenever there is a threat to personal liberty, even by a non-State actor.” Thus, while the cases analyzed in this study do not have guidance on enforceability, subsequent cases should be able to refer to *Kaushal Kishor* to protect the right to privacy of victims/survivors of OGBV, even against private actors.
Impact of new draft criminal law bills

At the time of publication of this report, the Central Government introduced three bills in Parliament—the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagrik Suraksha Sanhita, 2023, and the Bharatiya Sakshya Bill, 2023—to replace the current IPC, CrPC, and IEA, respectively. These laws seek to overhaul the criminal justice system. Initial analyses from experts have shown that the draft laws closely match current laws, but there are some updates to existing provisions and a few wholly new clauses. These laws, once passed, will also affect how OGBV gets addressed in courts and the criminal justice system. While we are cognizant that the new Bills—especially on OGBV and questions of electronic evidence—impact this study, we have retained our findings, without reference to the new Bills, in order to preserve potential lessons for the future. Overhauling a country’s criminal justice system must be an exhaustive and consultative process. It is our hope that these Bills will also see the full spectrum of public consultations and parliamentary scrutiny, and avoid the vagaries, vagueness, and language-oriented pitfalls of the current laws.

With these notes in mind, we move to the findings of the study that encapsulate the core of our research.
Chapter III: Findings

3.1 Finding 1: Gaps in the Indian judiciary’s understanding of the online public sphere based on its adjudication of OGBV

This study aims to assess OGBV cases in Indian courts. While analyzing the 94 cases before us, we witnessed several trends that are indicative of not just the limitations of the law but also the positive steps that the judiciary has taken in the last few years with regard to these offenses.

The OGBV cases we have studied include aspects of NCIID, threats of NCIID and intimidation, gender trolling, creation of fake accounts on social media, etc. These offenses were often combined with offline offenses like rape and sexual assault. Through these cases, we observed the following overarching trends specific to OGBV cases:

1. Absence of recognition of the online–offline continuum, and the real-world impact of online violence;
2. Lack of understanding of gendered hate speech, especially since legislations do not define this offense; and
3. NCIID as the prevalent and recurring offense across the cases studied.

3.1.1 The judiciary fails to recognize the online–offline continuum and tends to prioritize offline offenses in cases where both have occurred

As an increasing number of women access the cyberspace, there has been an analogous rise in cases of OGBV.48 There is nothing purely virtual about online violence, especially because its impact is increasingly spilling over into offline spaces, sometimes with severe consequences. Correlations between in-person abuse and OGBV have been documented through multiple studies, including one by UNESCO.49 In this study, 20% of women journalists reported having been the targets of offline abuse and attacks that they believe were connected with online violence they had experienced.

Despite such evidence, we found that Indian courts ignore the online–offline continuum along which OGBV takes place. The gravity of online offenses is disregarded until an offline offense occurs. Often, online harms result in offline offenses. In many cases where the accused is charged with committing both online and offline offenses, courts tend to focus more on the offline offenses.

In the case of Shmeer A v. State of Kerala,50 the accused trespassed into the house of the complainant, threatening to post her intimate images online and then raped her. In Raja Kumar v. State of Bihar,51 the accused administered an intoxicant to the complainant, recorded an intimate video of her, and subsequently demanded money from her to not circulate the video on social media. However, apart
from laying down the facts of the nature of the crime and observing that the social media video recorded and circulated belonged to the co-accused, the case does not make more mention of the seriousness of the crime. In *State v. Raj Babbar @ Raj*, and in *State v. Lalit Kumar (2016)*, the accused were tutors who assaulted their minor students and threatened to circulate their pictures on the internet. The *Raj Babbar* case has come to a stage of framing of charges and the court cannot go into the probative value of evidence lying before it because the prosecutrix, who is a minor, did not detail the sexual assault and termed it “*galat kaam*” (bad deed), instead. Due to this limitation, despite the accused having used a mobile phone to click pictures of the prosecutrix holding a beer and extorting money or favors after threatening to put these pictures on the internet, the court and its arguments have not focused on the online violence aspect of the case and focused, instead, on the interpretation of “*galat kaam*” and the offense of extortion. In the *Lalit Kumar* case, however, the judge has noted the call detail records (CDR) not being obtained to be added into evidence. At the same time, while acquitting the accused due to the prosecution’s failure to prove the case, the judge also instructed for a copy of the judgment to be sent to Commissioner of Police, Delhi, with directions to launch a proper probe into the “showdy [sic] investigation” of the matter by the police officials, particularly regarding electronic evidence, and send the court a copy of the action taken report.

Both these cases clearly demonstrate that despite the online–offline continuum on which cybercrimes take place, the online or the tech-facilitated aspects are not discussed in as much detail as the charges placed or incidents that have offline implications, such as the nature of the accusation, details of the sexual assault, etc.

One of the cases in our study particularly addresses the question of whether the online public sphere is considered a public place as per the Indecent Representation Act. In 2018, the Madras High Court presided over *Logeswaran v. State*. This case involved harassment in the form of a series of vulgar messages received by the victim/survivor via mobile phone while she was in her home. The court, interpreting the phrase “any other place” in Section 4 of the Tamil Nadu Prohibition of Harassment of Women Act, 1998, reasoned that the meaning of the phrase could not be extended to the home of the victim/survivor. The court observed that a detailed description in Section 4 signals that it should only be applied when harassment takes place in a “similar public place”. Therefore, the court reasoned, that messages sent through a mobile phone would not fall under Section 4 of the Tamil Nadu Prohibition of Harassment of Women Act. This interpretation points to the difficulty of establishing the boundaries of a public place in the context of digital communication. In this case, the court relied upon the physical location of the recipient of the message to understand if the space where harassment occurred was public. The court noted “that the harassment suffered in the case is within the confines of the home/place, wherein a computer is housed”. This is a strange observation, not least because the
message was received on a mobile phone and not a desktop that is unlikely to be moved around. A mobile phone is, by virtue of its definition, carried around everywhere, including public places. It is clear that existing interpretations of public place in law no longer hold true in a digital world and it is necessary for the judiciary to update its interpretation of these categories.55

One of the biggest hindrances in tackling online violence is that it is considered less serious or “less real” than offline crimes.56 Online violence is often treated as a non-corporeal crime, since the image that emerges is of mental trauma and not physical aggression. Herring explains that while we are accustomed to perceiving offline violence as harmful, online violence is “less prototypical” and is perceived as unintentional and fairly harmless.57 However, in reality, technology can accelerate or facilitate traditional human behavior and crimes against women. Additionally, online violence can have severe consequences as demonstrated by a study where the victim/survivor pleaded that every time she saw the content that constituted cyberviolence committed against her, “her whole body shivered and cringed”.58 Through threats and coercion, online violence could lead to violence or rape in the physical world, thereby creating “embodied harms”, and completing the continuum of violence against women, which ranges from “choice to pressure to coercion to force”.59 As Sharad Chauhan observes:

“Contrary to geospatial crimes, in techno-social crimes the extent, nature, and spread are unknown. The huge limitless formless online space creates a force multiplier effect where damage is done by multiple offenders on multiple victims, enjoyed by multiple beneficiaries, and tolerated by multiple bystanders.”

The cases we studied always had multilayered offenses with offline and online impacts. In several situations, threats to publish intimate content online coerced women to engage in non-consensual sexual activities in person. The impact of the online on the offline is not easy to separate. In fact, the separation between the two is false, and the fact is that the online–offline space is a continuum, replicating similar predicaments.

The online public sphere, an extension of the offline interaction, replicates the hierarchical structures of the offline.61 The two spaces feed off each other and can transcend from one to the other.62 Just as women have been facing backlash and violence when they enter traditionally ‘male spaces’, their participation online is also fraught with everyday sexism and violence, which is often minimized as something they have to deal with if they want to access social media.63 Women in courtrooms, in cases with elements of OGBV, face similar conundrums. The prevalence of this continuum necessitates cyber gender sensitization of the police and judiciary to help them understand the true scope of the problem and deal sensitively with the problem within the scope of the present laws.
3.1.2 The judiciary does not recognize online gender-based hate speech because the concept does not have statutory recognition

Through our study, we came across a variety of cases, including those of NCIID and intimate partner violence, but could not identify a single case referring to ‘online gender-based hate speech’ or ‘hate speech’. It is directed against a specific or identified individual or group. The group is identified on the basis of “an arbitrary and normatively irrelevant feature” (such as caste, gender, and religious identity). Hate speech vilifies or stigmatizes a target group, through disparagement and vilification, by implicitly or explicitly ascribing undesirable qualities to them that would make them the target of hostility or discrimination.

The Council of Europe’s (CoE) Additional Protocol to the Convention on Cybercrime defines sexist hate speech as, “expressions which spread, incite, promote or justify hatred based on sex”. In India, the 267th Law Commission Report defines hate speech as:

“Hate speech generally is an incitement to hatred primarily against a group of persons defined in terms of race, ethnicity, gender, sexual orientation, religious belief and the like (Sections 153A, read with Section 298 IPC). Thus, hate speech is any word written or spoken, signs, visible representations within the hearing or sight of a person with the intention to cause fear or alarm, or incitement to violence.”

Despite this proposed working definition, in practice, in India, hate speech is traditionally seen as a problem in relation to national security, terrorism, and public order. Even though two to three cases in our study fit the general qualifiers of the definitions of hate speech mentioned above and do, in fact, target a particular gender, the courts have not recognized them as such because Indian legislation on hate speech does not see it as an issue that affects gender.

In Sasikala Pushpa v. Facebook India & Ors, the plaintiff had alleged that the circulation of a photograph of her with a man from a rival political party was defamatory. The photos were uploaded on and circulated through social media, i.e., Facebook, Twitter/X, YouTube, and WhatsApp. The plaintiff argued that allowing further publicity to the content of such a photograph/video would only be for sensational and salacious purposes and would amount to a gross and irreparable violation of an individual’s privacy; it would be per se defamatory. This case was adjudicated keeping in mind ‘defamation’ provisions under the law. The focus of the adjudication was on the fact that the “public interest in knowing the meeting of the plaintiff at her residence with a man belonging to a rival political party far outweighs the private interest of the plaintiff of keeping the same hidden from public eyes”. In this civil suit for defamation, the aspect that is not considered is the gendered targeting to shame the woman.
In IT for Change’s study on misogynist trolling and abuse against Indian women in public–political life, the findings indicated that the subjects of the study, regardless of their political leaning, face substantial online violence on factors unrelated to politics. The abusive speech directed at women in public life rarely has anything to do with their work or stated political positions. It invariably takes the form of gendered attacks on their bodies or character. Rather than responding to or engaging with political positions (even with anger or abuse), trolls tend to question women’s credentials or trivialize their role in politics.\(^1\)

Two other cases that targeted women in the online public sphere but did not recognize it as being gender-based hate speech due to the statutory lacunae were also filed for civil remedies of compensation for the abusive speech. In the case of *Nimisha Bhagat v. Sneha Mahajan Nee Dogra*,\(^2\) the defendants engaged in mudslinging against the plaintiff on various Facebook groups. They created and posted provocative, derogative, and threatening comments on WhatsApp groups while also circulating the plaintiff’s phone numbers to strangers (doxxing), which led to her facing trolling. Defendants started to misuse social media platforms by posting selective sections of video recordings, prompting and instigating others to send violent, abusive, threatening, and derogatory responses, thereby defaming the plaintiff. Defendants managed to elicit unwarrantedly abusive, repulsive, and threatening posts/responses from their several Facebook friends. This alarmed the plaintiff about her life and safety. This was a case for recovery of damages and an injunction to prevent further hate online although it has elements of hateful behavior, vilification, and targeted abuse. Additionally, the court noted:

> “The fundamental right of speech and expression does not cover abusive, threatening and vituperative messages on social media sites or otherwise. Therefore, the stand of the defendants, as set out in their pleadings, that their fundamental right to freedom of speech and expression justifies it cannot be accepted.”

In the case of *The Present Petition Has Been … v. Unknown*,\(^3\) a bail appeal for a case of gender trolling, the petitioner used his Facebook and Twitter/X accounts to spread fake and scandalous news against women (more women belonging to the media). The court rejected the anticipatory bail request stating that in such a case the “larger interest of the public” required consideration “as opposed to the demand of individual liberty”.

Thus, gendered hate speech not having statutory recognition in India can be directly linked to the lack of such cases in our sample set. Even the examples given above are either defamation cases or civil suits seeking injunctions to prevent abuse. Since the Indian legislative intent for hate speech is oriented towards the redressal of ‘promoting enmity’ between communities, gendered and misogynistic hate is often overlooked. There is a need to acknowledge that online violence faced by
women and non-binary people is usually based on their gender, an extension of the violence they face offline as well. As per international practice, in the European Union (EU), for instance, different areas of law provide protection against hate speech and hate crime and this might be due to the fact that the terms ‘hate speech’ and ‘hate crime’ do not have universal definitions and, thus, are interpreted differently by the member states. In Greece, applicable legislation uses synonyms while referring to the concept of hate crime. The synonym used here is racist crime, which is a crime committed due to a hateful bias on the grounds of race, color, religion, descent, national or ethnic origin, sexual orientation, gender identity, or disability of the victim/survivor. In Hungary, hate crime and hate speech are defined in existing literature and are commonly used in practice. A hate crime is defined as a crime committed based on a biased motive against a certain group. Meanwhile, hate speech refers to a behavior that may offend, harass, or intimidate other people on the grounds of their protected characteristics, such as skin color, ethnicity, nationality, sex, religion, etc. Greece seems to be the only member state assessed that specifically mentions gender identity in its hate speech legislation.

Currently, there is a gap in both knowledge and policy action even at the global level to combat sexist hate speech. A step forward has been taken by the CoE’s Gender Equality Strategy 2014–2017, which explicitly includes tackling sexism as a form of hate speech under its strategic objectives. The 267th Law Commission report also provides hope for such recognition, but this must happen at the earliest, as neither the internet nor misogyny are going away any time soon.

### 3.1.3 Majority of the cases of OGBV within this study relate to NCIID and use legal provisions that are patriarchal in their construct

One of our primary observations was the recurrence of NCIID across most of the cases in our sample. “Non-consensual distribution of intimate images occurs when someone shares an intimate image, usually an image of another person in the nude or engaging in sexual activity, without that person’s consent”, usually shared with “friends, employers, and family members of the person in the images in an effort to humiliate that person”. Out of our list of 94 cases, 71 (~75%) had an element of non-consensual sharing of intimate images. These included cases where men committed sexual assault on women by threatening to publish their intimate or personal images, which were, in many cases, taken without consent. It is relevant to note that the Indian law does not recognize the phrase ‘non-consensual intimate image sharing or distribution’. Instead, there are a combination of legal provisions that can be used to address these cases. For our purposes, we ascribed the tag of NCIID to any case where an image-based offense—in the form of non-consensual sharing or threats using such an image to blackmail the victim/survivor—had taken place in our sample.
We analyzed the NCIID cases from our sample based on two axes:

1. The various legal provisions used to prosecute NCIID cases under Indian jurisprudence; and
2. the prevalence and frequency of application of particular provisions of law to such cases and the reasons to do so.

These have been explained in greater detail in the following sections.

### 3.1.3.1. Legal provisions used to prosecute cases of NCIID

Since the Indian law does not recognize the phrase NCIID, provisions of voyeurism under the IPC or violation of privacy (in a limited definition of physical privacy) under the IT Act are used in cases where sensitive images of women are taken and/or transmitted on the internet without their consent. Given that we used legal provisions to shortlist potential cases of OGBV, the number of times these provisions were used became a good indicator to understand which laws were used in cases of NCIID. Aside from the provisions chosen to shortlist cases, which have been mentioned in the methodology section (see section 2.2.3), several other legal provisions showed up on the list of cases. Outside of the IPC, the IT Act, and the Indecent Representation of Women Act, which were the primary laws we focused on to arrive at the sample set of cases, laws like the Protection of Children from Sexual Offences Act (POCSO), the Scheduled Castes and Scheduled Tribes (Prevention of Atrocities) Act, and the Tamil Nadu Prohibition of Harassment of Woman Act, 1998 also came up.

The 10 most frequently invoked provisions of law that are used in OGBV cases, specifically when image-based abuse is identified, have been listed in Table 3.\(^1\) The reasons for the prevalence of some of these provisions have been discussed in the following section.

<table>
<thead>
<tr>
<th>Specific provisions</th>
<th>Short title of the provision</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPC 506</td>
<td>Punishment for criminal intimidation</td>
</tr>
<tr>
<td>IPC 376</td>
<td>Punishment for rape</td>
</tr>
<tr>
<td>IT Act 67</td>
<td>Punishment for publishing or transmitting obscene material in electronic form</td>
</tr>
<tr>
<td>IT Act 67A</td>
<td>Punishment for publishing or transmitting material containing sexually explicit acts, etc., in electronic form</td>
</tr>
</tbody>
</table>
3.1.3.2. What do the frequently invoked provisions of law in cases of NCIID indicate?

In our sample set of cases, punishment for criminal intimidation was invoked the highest number of times, indicating that online violence is often used as a means of threatening victims/survivors. The next highest frequency of a provision being used was that of punishment for rape, which was absent in our initial shortlist of provisions for potential OGBV cases, providing evidence that there is a close connection between online violence and offline violence. A lot of the other provisions in Table 3 are related to outraging modesty, obscenity, sexually explicit material, etc. The relevance of these types of offenses emerging in our study has been discussed below.

1. **Criminal intimidation:** As mentioned above, our list of NCIID cases included cases where the victim/survivor was threatened with the publication of their intimate photographs online. We observed through the cases that the offense of criminal intimidation straddles the fine line between online and offline spaces. Further, the vast potential of the internet to spread intimate images, and the potential impact of such virality, creates a potent threat that can lead to coercion on many levels. For instance, in *Shemeer v. State of Kerala*, the bail petitioner, charged with criminal intimidation, was accused of taking nude photographs of the victim/survivor, threatening her of uploading the same on social media, trespassing into her house, and raping her.

2. **Real-world impact of threats to publish intimate photos online:** Our cases show that threats to publish intimate photographs online are a common way to exploit victims/survivors and coerce them into sexual activity. At present, the redressal for such an offense is through the criminal intimidation provision. However, a provision akin to Section 91R of the New South Wales Crimes Act, introduced in 2017, which specifically criminalizes threats to record or distribute intimate images without consent may offer a specific solution in this case, given the

---

| IPC 354C | Voyeurism |
| IPC 292 | Sale, etc., of obscene books, etc. |
| IT Act 66E | Punishment for violation of privacy |
| IPC 354 | Assault or criminal force against a woman with the intent to outrage her modesty |
| IPC 509 | Word, gesture, or act intended to insult the modesty of a woman |
| IPC 354D | Stalking |
proliferation of the digital in today’s world. It also clearly indicates the online–offline continuum discussed earlier in this chapter. This is not to say that purely online offenses have any less impact. Online gender-based offenses are known to affect the mental health of survivors, often leading to “stress, anxiety, panic attacks, powerlessness, and loss of confidence”. However, it is important to recognize that none of these offenses occur in siloes, and the online public sphere is as real and impactful, if not more, as its offline counterpart in cases of gendered violence.

3. **Patriarchal construct of NCIID provisions:** The phrase NCIID has been coined centering consent and divested of moral judgment. In fact, as early as in 1983, Catharine MacKinnon and Andrea Dworkin, proposed an antipornography civil rights ordinance, which sought to distinguish the harms suffered by women as opposed to framing them within the concepts of ‘obscenity’ and ‘immorality’. However, Indian legal provisions on the matter are far from being so. In the Indian context, legal provisions to address NCIID (see Table 3) often focus on the offense ‘outraging the modesty’ of the woman, publishing or transmitting obscene material, or a sexually explicit act. Even the violation of privacy provision under Section 66E is narrowly constructed, and relates primarily to physical or bodily privacy. Going by the morality inherent in conceptions of modesty, and the framework of image-based violence laws proposed by MacKinnon and Dworkin, it is easy to witness the fact that the language of the laws is not rights-focused but tends to emphasize patriarchal ideas.

Cases of OGBV in courtrooms are, in many ways, evolving, even if they may be a little behind the technology of our times. The sections above are proof that there are nuances within the broad scope of OGBV that need to be identified for the judiciary to be able to offer justice to the victims/survivors of OGBV. Our initial analysis of OGBV within our sample set offered insights into addressing some of these nuances, including:

1. Issues of sexism in courtrooms;
2. the lack of emphasis on the right to privacy of the victim/survivor as the core violation;
3. the need to govern social media and seek accountability;
4. the concerns around the criminal justice system; and
5. the recognition of existing power differentials.

The following chapters delve into greater detail about each of these.
3.2 Finding 2: Courts have increasingly begun to recognize and implement the right to privacy in OGBV cases, following the *Puttaswamy* ruling of the Supreme Court in 2017

The right to privacy has been much contested and debated in the Indian judiciary since the 1950s, especially because it was not a part of the fundamental rights in the Constitution of India. Over the years, though, it has not only become a cornerstone of dignity of individuals, but has also been declared a fundamental right necessary for life and personal liberty as affirmed in 2017 by a nine-judge bench of the Supreme Court in the *Puttaswamy* case.87

“Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution. Elements of privacy also arise in varying contexts from the other facets of freedom and dignity recognised and guaranteed by the fundamental rights contained in Part III.”

In this manner, the right to privacy has become an inherent and fundamental right of an individual. It includes three groups of rights:88

1. Informational privacy, which relates to control of personal data;
2. physical privacy, which is the right to bodily integrity against unlawful intrusions; and
3. decisional privacy, which offers protection to the personal autonomy of a person from various kinds of unreasonable external influence.

Privacy is also one of the three core principles in understanding the rights of women and gender minorities in cases of OGBV. These three principles—equality, dignity, and privacy—are significant to the central argument of this study.

Indian legislations have also occasionally referred to privacy, like in Section 66E89 of the IT Act, Section 50990 of the IPC, and more recently, Section 354C91 of the IPC. All of these provisions have a limited scope of what privacy means. It is mostly defined through references to a woman’s body, ‘private areas’, or ‘modesty’. This is a protectionist approach that focuses on the woman’s body rather than her rights. It does not provide a holistic reading of privacy as discussed above and negates women’s agency.92 Narrow definitions of privacy are no more in consonance with India’s fundamental rights jurisprudence, as discussed in the following sections.

Arguably, fundamental rights are not enforceable against private parties, as discussed earlier in this study. However, the Supreme Court93 has recently enabled this—i.e., made it enforceable against non-state actors—in the case of Article 21. It is a forward-looking move that will help cases of OGBV, since
they are often criminal cases dealing with questions of individuals’ privacy. In that regard, the positions within this chapter reflect the direction cases could take in the future.

In the study, we have also attempted to understand the frequency with which privacy is mentioned and its understanding, especially in cases of OGBV. As mentioned in earlier chapters, a large set of these cases revolve around NCIID, which is an inherent violation of privacy of the woman victimized by these offenses. The key finding here helped us identify whether courts recognize the right to privacy in cases of NCIID and similar offenses.

For the purposes of this study, and this section in particular, we consider cases to be privacy violations when one of the following offenses have taken place:

1. Non-consensual sharing of intimate images or videos;
2. Creation of morphed photos or fake profiles; and
3. Sexual violence based on non-consensual intimate images and threats to distribute them.

Based on the points listed above, two key questions arise that have been analyzed in the following sections.

1. Is privacy understood as an inherent right being violated or is it only in cases where such a right is expressly identified (as in Section 66E or the Kerala Police Act provisions)?
2. Do courts identify informational privacy or do they understand privacy as a limited bodily construct (as in the phrasing of 66E)?

3.2.1 While the Puttaswamy ruling recognizes privacy as an inherent right, courts adjudicating OGBV cases rely on paternalistic concepts like modesty and honor

The Puttaswamy verdict is a landmark decision not only for its recognition of the fundamental right to privacy but also because it offers a holistic and interconnected framework of the right to privacy, one that connects privacy with the fundamental right of equality and the right to life with dignity. The decision paved the way for the set of rights that we believe protect the rights of individuals in cases of OGBV. Our study shows that cases that discuss privacy after 2017 have done so on the foundation of the Puttaswamy verdict. Cases referring to privacy pre-2017 rely on legal provisions that specifically mention privacy, like Section 66E of the IT Act or Section 509 of the IPC. However, even in cases where there is an explicit recognition of the violation of privacy, we wanted to understand how courts refer to it and whether their perspective is progressive or paternalistic.

Non-consensual distribution of intimate images, one of the largest types of cases observed in our study, can be a traumatic experience for the victims/survivors. Data from an IT for Change survey suggests that from a total of 326 respondents who suffered from various forms of online violence, 30%
have been victims/survivors of NCIID.\textsuperscript{95} Similar numbers (28.5\%) were noted in another study conducted at a Canadian university.\textsuperscript{96} However, in most cases, the language of the laws protecting against this offense is often based on patriarchal stereotypes of morality and modesty. “Outraging the modesty of a woman” is a Victorian refrain that has remained in Indian statute books (Section 354,\textsuperscript{97} and Section 509). These provisions are also frequently used in cases of NCIID. While privacy has been introduced in the IPC through Section 354C and Section 509, in the IT Act through Section 66E, or through the Kerala Police Act, these are often reduced to refer to “private areas” of the body or a woman’s modesty. It is also curious that while courts often refer to a woman’s modesty, there is no legislative definition of modesty available as such. The definitions that are available are through judicial pronouncements and based on common parlance, which relies on patriarchal tropes.\textsuperscript{98}

In 1966, the Supreme Court, while hearing a case of sexual assault of a 7.5-month-old infant, noted, “The essence of a woman’s modesty is her sex. Even a female of tender age from her very birth possesses the modesty which is the attribute of her sex.”\textsuperscript{99} Subsequent cases have looked at the Oxford Dictionary for a definition of modesty—including, “womanly propriety of behavior: scrupulous chastity of thought, speech and conduct (in man or woman); reserve or sense of shame proceeding from instinctive aversion to impure or coarse suggestions”\textsuperscript{100}—or interpreted these together to arrive at “the ultimate test for ascertaining whether modesty has been outraged”, i.e., “the action of the offender such as could be perceived as one which is capable of shocking the sense of decency of a woman”.\textsuperscript{101}

Given this archaic understanding of modesty, it clearly cannot serve as the benchmark on which gendered offenses can continue to be judged. Unfortunately, it was evident through our study that courts tend to take the modesty approach even today. Against this backdrop, we argue that violation of privacy, when defined holistically, becomes a better measure or benchmark to test offenses as opposed to traditional notions of modesty.

The Puttaswamy decision is a significant verdict on privacy, which moves the definition beyond the realm of mere bodily privacy to one that recognizes dignity and inviolable rights. The Supreme Court noted:

“Privacy enables the individual to retain the autonomy of the body and mind. The autonomy of the individual is the ability to make decisions on vital matters of concern to life…Privacy of the body entitles an individual to the integrity of the physical aspects of personhood. The intersection between one’s mental integrity and privacy entitles the individual to freedom of thought, the freedom to believe in what is right, and the freedom of self-determination… Above all, the privacy of the individual recognises an inviolable right to determine how freedom shall be exercised.”

The court also stated, “Privacy safeguards individual autonomy and recognises the ability of the individual to control vital aspects of his or her life…Privacy attaches to the person since it is an
essential facet of the dignity of the human being.” Couched in these terms, the recent decisions discussed below have been open to recognizing violation of privacy in cases of NCIID.

The case of Subhranshu Rout v. State of Orissa\(^{102}\) is a bail application where the Odisha High Court was cognizant of the privacy of the victim/survivor in a case of NCIID. The accused (and bail applicant) was charged with rape and posting a video of the victim/survivor on a Facebook profile. Despite being a case of bail under Section 439 of the CrPC, the court recognized the victim’s/survivor’s right to privacy and delved into the right to be forgotten. The court denied bail on the grounds of the “heinousness of the crime” and added:

“As in the instant case, the rights of the victim to get those uploaded photos/videos erased from Facebook server still remain unaddressed for want of appropriate legislation. However, allowing such objectionable photos and videos to remain on a social media platform, without the consent of a woman, is a direct affront on a woman’s modesty and, more importantly, her right to privacy. In such cases, either the victim herself or the prosecution may, if so advised, seek appropriate orders to protect the victim’s fundamental right to privacy, by seeking appropriate orders to have such offensive posts erased from the public platform, irrespective of the ongoing criminal process.”

The case of X v. YouTube\(^{103}\) is significant because it was filed as a civil suit with a claim for right to be forgotten and sought relief under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules, 2021), which required platforms to remove objectionable content within 24 hours of receiving a complaint. The case related to explicit videos the plaintiff had consented to be in part of, but later withdrew consent from the producer to publish them. However, other websites took the content and continued to distribute them. In 2021, the Delhi High Court provided interim protection to the victim/survivor and ordered the defendants to remove content that violated her privacy, given that she had not consented to them being shared. The court noted:

“Following the view taken by a co-ordinate Bench of this court in Zulfiqar Ahman Khan[...][that the ‘right to privacy’ includes the right to be forgotten and the right to be left alone as ‘inherent aspects’, this Court is also of the opinion that the right to privacy of the plaintiff is to be protected, especially when it is her person that is being exhibited, and against her will. In the circumstances and in view of the fact that the plaintiff is entitled ‘to be left alone’ and ‘to be forgotten’, she is entitled to protection from invasion of her privacy by strangers and anonymous callers on account of such publication/streaming/transmission of the suit videos by the defendants.”

The court also clarified that even if the plaintiff had consented to participate in the filming of the videos, the fact that she had not licensed other websites to distribute them was sufficient to restrain them from profiting off these explicit videos while the case was pending.
The above cases are examples where the court explicitly relied on the fundamental right to privacy of a victim/survivor of OGBV in NCIID cases. However, there is still a long way to go to a scenario where the right to privacy becomes the sole reason a victim/survivor receives protection in cases of online violence in the nature of NCIID, morphing, etc. In fact, some of the cases in this study, discussed in the following paragraphs, referred to privacy but had a paternalistic tone towards the victim/survivor. This is reflective not of the absence of explicit recognition of the right to privacy, even in statutes, but a need for judicial training that divests moral considerations from questions about the rights of victims/survivors.

The case of Smt. Qamar v. State of Telangana is a writ petition filed by the mother of an accused person in preventive detention under the Telangana Prevention of Dangerous Activities Act, 1986, on grounds of being a “sexual offender” and restraining him from committing further offenses. The writ petition claimed that despite getting bail in all three cases, the police filed an illegal detention order against the accused, which was confirmed by the state government. The Telangana High Court recognized the harm to a woman’s right to privacy when intimate images were published without her consent, but also brought in concepts like “honor” and “sanctity of a female”. It quashed the writ petition, challenging a detention order against the accused, and noted:

“Sexual violence against women, apart from being a dehumanizing act, is an unlawful intrusion into the right to privacy and sanctity of a female. It is a serious blow to her supreme honor and offends her self-esteem and dignity. It degrades and humiliates the victim and leaves behind a traumatic experience. The Courts are, therefore, expected to deal with cases of sexual abuse against women with utmost sensitivity.”

This perspective of the court, especially to be sensitive in cases of sexual violence is commendable. However, the language used is not rights-oriented but rather relies on tropes of honor and morality. The court, in its order, continued:

“Sexual abuse not only violates the victim’s privacy and personal integrity, but inevitably causes serious psychological as well as physical harm. A murderer destroys the physical body of the victim, but a sexual assaulter degrades the very soul of a helpless female. The Courts, therefore, shoulder a great responsibility while trying an accused on charges of sexual abuse. Sexual abuse against women needs to be dealt with sternly and severely. To show mercy in such heinous crimes would be a travesty of justice and the plea for leniency would be wholly misplaced.”

The court dismissed the writ petition and held that the preventive detention order was valid in protecting public order and restraining the accused from committing further offenses. While fair trial arguments remain valid in the face of the power of the state in the criminal justice system, creating avenues to protect victims/survivors of sexual offenses, including the ones committed online, is
significant. However, to do so in a way that treats survivors as “helpless females” enables the same patriarchal spaces in courtrooms that have been highlighted in numerous studies before this.

The case of Guruvinder Singh v. State of Uttar Pradesh\textsuperscript{105} is also significant because the Allahabad High Court unequivocally stated that the role of the court is to act as a guardian of a woman’s rights, which is admirable. It also referred to the right to privacy guaranteed under the fundamental rights because of the Puttaswamy verdict. The case was a bail application by a person accused of rape and making explicit videos, which were then used to continue to coerce the victim/survivor. Additionally, the accused also sent explicit photographs to the victim’s/survivor’s mother and sister. The court did rely on some tropes of “outraging the modesty of the woman” and observed:

“No person much less a woman would want to create and display gray shades of her character. In most of the cases, like the present one, the women are the victims. Capturing the images and videos with consent of the woman cannot justify the misuse of such content once the relation between the victim and accused gets strained as it happened in the present case. In matters like the present one, any accused will surreptitiously outrage the modesty of the woman and misuse the same in the cyber space unhindered.”

However, the court also focused on the rights of the victim/survivor in this case. Denying bail to the accused, the court added:

“It would be appropriate to observe that the sexually explicit images or videos may be made by a partner of an intimate relationship with the knowledge and consent of the subject, or it may be made without his or her knowledge, however, the same if used as a form of revenge or harassment would definitely distort/damage the dignity of concerned and the court in such type of cases cannot close its eyes and being parens patriae and protector of fundamental rights, the court should come forward to protect the right of the subject and similarly the court should stringently deal with the person concerned.”

What this case reflects is the ability of high courts to invoke their role as protectors of fundamental rights, like the right to privacy, in cases of OGBV to protect victims/survivors. Additionally, it shows that while patriarchal overtones persist in the language of the courts, it is possible to rely on a rights-based approach to decide cases.

Of the cases that do discuss privacy, ones like Guruvinder Singh or Subhrangshu Rout stand out, as they refer to privacy within the ambit of the fundamental right to life under Article 21, as per the Puttaswamy decision. This is a significant development and a step in the right direction for cases of OGBV, especially where there is a breach of consent and violation of privacy of an individual through NCIID.
Within the ambit of our research, there are several other cases, largely criminal ones, of various types of online violence, where a violation of privacy has taken place, but the courts do not recognize them as such. A primary reason for this could be that the provisions of law under which these cases have been filed—like Section 354D (stalking), Section 67 (publication of obscene material), Section 67-A (punishment for transmitting sexually explicit material) of the IT Act or provisions of the POCSO Act—do not refer to violation of privacy explicitly. This reflects a gap in the legal system where privacy violations are not recognized as an offense or breach on their own.

In criminal cases, it is significant to use provisions that explicitly mention privacy, especially for a subordinate court to take cognizance in the first instance. Concerns then arise about whether the right provisions are being used at the stages of registering an FIR (first information report), filing a charge sheet, or framing charges. In some cases, the facts may not allow for a privacy-based offense to be applicable because of the limited definitions of these offenses. However, the cases discussed above show how high courts are able to reflect on the fundamental right to privacy being violated in cases of OGBV and base their decisions on them. This is a step in the right direction. Additionally, now that the Supreme Court has declared Article 21 to be enforceable against non-state actors, it enables survivors to enforce the right to privacy against private actors, including platforms and the accused in certain criminal cases, to either take down illegal material that may have been published or distributed. It remains to be seen how that jurisprudence develops. We acknowledge that this necessitates courts to be activist in their approach, and in criminal cases that can often be to the detriment of the accused. However, in the absence of laws that meet the needs of the day, courts are required to balance the rights of victims/survivors and the accused.

3.2.2 Courts tend to understand privacy narrowly rather than holistically, which includes informational, physical, and decisional privacy

How do courts understand privacy and do they recognize issues of informational privacy? Informational privacy, as mentioned before, refers to control over one’s personal data. This could include information like one’s phone number, residential address, place of work, etc. In the cases studied, issues of doxxing or revealing personal information of individuals were not prevalent. There were cases where fake social media or matrimonial website profiles were created.

In most of the cases in this study, online violence was often of a sexual nature. In such cases, courts were limited to the physical privacy of the individual. While many courts were cognizant of the mental anguish these cases can cause, those overlapping with recognition of privacy violations were few. For example, even in X v. State & Ors, the Delhi High Court directed online intermediaries to remove content that qualified as child pornography because of non-consensual distribution of a teen girl’s photographs. However, the question of violation of her privacy did not come up. Similarly, in
Mohammad Nasar v. State of Andhra Pradesh, the Andhra Pradesh High Court denied anticipatory bail to the accused against whom there were multiple complaints of NCID. Again, the violation of privacy was not a consideration, even though the court was cognizant of the seriousness of the offense. In cases where there was no sexual element or the case was purely an informational privacy-related issue, courts had other considerations. The Delhi High Court, in Sasikala Pushpa v. Facebook India, did not recognize an inherent right to privacy over one’s photographs, or informational privacy, especially if they are part of public life. The plaintiff in the case had alleged that the circulation of her photograph with a man from a rival political party was defamatory. The court considered whether the photographs were defamatory or morphed, forged and fabricated to decide if their circulation could be valid, but did not find the content to be defamatory or violating her privacy. The court held, “The public interest in knowing the meeting of the plaintiff at her residence with a man belonging to a rival political party far outweighs the private interest of the plaintiff of keeping the same hidden from public eyes.” However, it is noteworthy that if the legal system identified the sanctity of informational privacy, a case could have been initiated under that provision.

The jurisprudence on issues like NCID has a checkered presence globally. Several countries have witnessed litigation against this type of online violence. For instance, in the Philippines, 42 perpetrators of different kinds of OGBV were indicted or brought to trial in 2021. In South Korea, a series of amendments were made to criminal and civil laws to account for widespread online violence against women and children, informally known as the ‘Nth rooms Prevention Act’. However, the holistic notion of privacy to protect the rights of a victim/survivor are at a nascent stage. Provisions like Section 33 of the UK Criminal Justice and Courts Act criminalize the disclosure of “private sexual photographs and films” without the express consent of the person in them and with the intent to cause them distress. While this provision is devoid of a paternalistic tone per se, the requirement of an “intent to cause distress” takes away from an individual’s right to privacy. For the EU, informational privacy is now also protected under the General Data Protection Regulation. However, in cases of OGBV, considerable developments are still required.

The key takeaway from this discourse is the need for a holistic and rights-based approach towards OGBV. In the context of Indian jurisprudence, this approach can be rooted in the right to privacy. It is imperative that the superior courts—both the Supreme Court and the state high courts—emphasize the role of privacy in cases of OGBV, as an increasing number of such cases have begun to come before courts. This will allow a fair, just, and equitable jurisprudence to develop, one that is separated from patriarchal notions and paternalistic overtones of modesty and obscenity.

As a demonstrative example, take the case of Robin Sharma v. State of Punjab from our study. In this case of anticipatory bail against various forms of online violence, the Punjab and Haryana High Court
noted the necessity for prompt investigation, especially in cases of, “unwanted intrusion into privacy of a woman”. The recognition of a holistic right to privacy will ensure that survivors can receive justice based on their dignity rather than outdated notions of morality. The Puttaswamy decision provided a great path to achieve this, and while courts have begun this journey, there is still a lot of ground to cover.

3.3 Finding 3: OGBV cases illustrate concerns of digital evidence and lack of understanding while issuing specific bail orders, reflecting challenges arising due to emerging technology within the criminal justice system

Cases of OGBV are governed by the criminal jurisdiction of courts. Most offenses are recognized by the IPC as well as the IT Act. This leads to the burden of proof—the responsibility of the prosecution to prove a charge—in these cases being much higher. Thus, evidence is key to prove the guilt of a perpetrator in these cases, leading to a high burden of proof. Several cases from our study could not meet this threshold. Consequently, they were not considered cases of OGBV. For example, in State v. Azhar Ali Bhutto, the judge noted, “Mere suspicion, however strong or probable it may be, is no effective substitute for the legal proof required to substantiate the charge of commission of a crime and [the] grave[er] the charge is greater should be the standard of proof required.”

Several challenges—including bringing in expert testimony, relying on witnesses, offering the right documentary evidence, and more—hinder an effective outcome of justice. For instance, in the case of State of Karnataka v. Sudeep, the prosecution failed to bring in an expert witness to prove that the accused created a fake account. The court noted, “[The] prosecution has not showed any person in the list of witnesses, who is well versed in ascertaining the aspect as to in what way the fake account has been created and by using which IP address the alleged messages have been sent to PW1 etc.” In essence, evidence plays a key role in criminal cases, and in online gender-based offenses, these are often digital in nature. There are unique challenges to electronic evidence that we noticed in our sample of cases, which have been discussed in section 3.5.

Aside from issues of evidence, another key theme that emerged from our analysis of the cases was of bail-related concerns. It appears that a lot of cases of OGBV, especially at the high court level, are at initial stages of bail. These bail orders reflect the gap between the general understanding of online gendered violence as opposed to its actual impact. While bail must be the rule in criminal cases, it may be necessary to implement some bail conditions in cases of online violence to reduce harm. Based on the insights from our sample that included bail, anticipatory bail and some trial cases, we were able to identify two main issues in cases of OGBV:
1. Difficulty in access and admission of digital evidence; and

2. sexist bail reasonings and bail conditions that do not keep the online public sphere in mind.

3.3.1 Courts do not uniformly recognize digital evidence in OGBV cases and often reject cases at a preliminary level because of certification requirements

The foundation for a sound criminal trial rests on the evidence produced to prove the charges against the accused. This evidence can be based on testimony (through witness statements) or documentary. After the enactment of the IT Act in 2000, the Indian Evidence Act (IEA), 1872, includes electronic records in its definition of evidence. This has had far-reaching impacts and continues to become more relevant in today’s rapidly digitizing world.

Digital evidence or electronic evidence is crucial in cases of OGBV, since the record of the wrongdoing or harm caused is captured on a device or the internet. Through the course of this study, we found several trial court cases where digital evidence played a role. The challenges faced while introducing digital evidence have been captured below.

‘The internet never forgets’ has become a common adage. However, when it comes to evidentiary value of electronic evidence in the Indian context, the collective memory of the internet seems to be valid only under one of two complicated circumstances:

1. If the original computer source is produced as primary evidence; or

2. if copies of the electronic record—printed on paper, stored, recorded or copied in CDs, etc.—supported by a certificate, under Section 65B of the IEA, are provided as secondary evidence.

These provisions, especially Section 65B, are so expansive that the Supreme Court has referred to them as a “complete code in itself”. The text of Section 65B(4), which specifically deals with the certificate, has been reproduced below.

“In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,

(a) identifying the electronic record containing the statement and describing the manner in which it was produced;

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate,
and purporting to be signed by a person occupying a responsible official position in relation to
the operation of the relevant device or the management of the relevant activities (whichever is
appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this
sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief
of the person stating it.”

The way to produce electronic evidence before courts, especially regarding the requirement of the
Section 65B(4) certificate, has been settled through two important Supreme Court cases: Anvar P.V. v.
P.K. Basheer122 and the more recent Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal.123 In Anvar,
a case of electoral impropriety, the failure to provide this certificate rendered all of the evidence
adduced invalid. The Supreme Court stated that this could have been avoided by including the original
or primary evidence, “by making available evidence, the CDs used for announcement and songs (of
alleged objectionable content)”. The Supreme Court clarified that the process for producing the
Section 65B(4) certificate ensured the source and authenticity of the electronic evidence, given that
digital evidence is “more susceptible to tampering, alteration, transposition, excision, etc. without
such safeguards, the whole trial based on proof of electronic records can lead to travesty of justice”.

The Khotkar verdict clarified the position of the certificate as being necessary but only for secondary
evidence. In this case, the Supreme Court established that especially in cases where a certificate is
demanded but not provided by an authority or person, the requesting party can apply to the court to
receive this certificate. Additionally, it noted the power of courts under the CrPC to direct that the
Section 65B(4) certificate be produced, to enable accessing the electronic evidence. It also overturned
the decision made by a smaller bench of the Supreme Court124 in an earlier case, Shafhi Mohammad v.
State of Himachal Pradesh.125

It is also interesting to note that this provision is drawn from Section 5 of the UK Civil Evidence Act
1968,126 which was repealed in the UK in 1995.127 In this context, the Indian law on electronic evidence
(included by an amendment nearly 20 years ago, before the recent technological developments) is
quite antiquated, especially where it refers to the “source computer” used to generate and process this
information. Although court decisions and interpretations have granted clarity regarding electronic
evidence now, it still does not compare to the more updated provisions in some other legal systems.
For example, in the concurring decision for Khotkar, Justice V. Ramasubramanian noted that the 2017
amendment to the US Federal Rules of Evidence128 has ensured that, “A lot of options have been made
available to litigants seeking to rely upon electronically stored information[…]This development of law
in the US demonstrates that, unlike in India, law has kept pace with technology to a great extent.”

Additionally, it must be mentioned that digital evidence can be a significant threat to privacy, since
devices and other material (including recordings, photographs, videos, and text threads) are expected
to be turned over to the State, largely the police or the court, and there are no safeguards per se on how this material will be used, and how the rights of the complainant will be protected. Tarun Tejpal receiving two years’ worth of private text messages and photographs sent by the prosecutrix who accused him of sexually assaulting her is demonstrative of this issue. Tejpal was provided more evidence than he had officially requested, which had only been the prosecutrix’s data for a period of about 1.5 months. In essence, the defense in this case was able to use the State’s resources to access personal communication that far exceeded what was necessary for the purposes of building their case. In fact, the court also used these extensive chats, especially private chats unrelated to the incident, to determine the character of the prosecutrix. This was significant because the court held in favor of Tejpal and acquitted him of all charges. This gap also needs to be addressed, especially in cases of sexual violence.

Two developments in the Indian legal system will impact concerns around data access by law enforcement and the concept of secondary digital evidence—the Digital Personal Data Protection Act (DPDPA) and the proposed law on evidence, which was introduced in Parliament in August 2023. The DPDPA provides a blanket exemption for processing personal data in relation to “prevention, detection, investigation or prosecution of any offense”. This does not safeguard privacy or rights of the complainant in any material way. The draft bill overhauling the IEA, known as the Bharatiya Sakshya Bill, 2023, is an improvement on electronic evidence, which no longer has the division of primary or secondary evidence. While a step in the right direction, it retains the requirement of a certificate to be provided alongside it in a form included as part of the bill. This is a step in the right direction; however, until this bill becomes law, it is imperative to discuss the concerns with the IEA as it stands today.

For the purposes of our study, we reviewed the subordinate court cases across Delhi and Bengaluru district courts within our sample to understand the role of digital evidence and the law governing it. Our sample set included several trial court decisions related to OGBV, which dealt with digital evidence. Through these cases, we noticed three broad categories of cases:

1. Cases where no certificate was asked;
2. cases where the court dismissed evidence due to the lack of a certificate; and
3. cases where digital evidence was not considered.

The following sections will discuss each of these in detail. It must be noted that there were a few cases where the Section 65B certificate was duly produced and the evidence considered. These have not been included below for the sake of brevity.
3.3.1.1 Cases where no certificate was asked

The first set of trial court cases were ones where courts reviewed the digital evidence but did not require the Section 65B(4) certificate. This was in keeping with the requirement that in case of primary electronic evidence, like mobile phones or computers, being produced, no certificate would be required. This reflects the position, established by the Anvar verdict in 2014, that only secondary electronic evidence will need the certificate. This is a straightforward position of law and, as such, causes no concerns for the judicial process in cases of OGBV.

3.3.1.2 Cases where the court dismissed evidence for lack of Section 65B(4) certificate

The electronic evidence in this set of cases was not considered by the courts because the requisite certificate was not produced with the evidence. The landmark case of Khotkar emphasizes the role and power of courts, under the CrPC, to call for such evidence. However, the cases in our study did not have any examples of this verdict being applied, likely because most of these cases were decided before Khotkar in 2020.

1. In State v. Lalit, the accused was charged with harassing a minor by calling her and sending messages. The photocopies of these messages and the CDR of a particular mobile number were not considered by the court for lack of an accompanying Section 65B(4) certificate. The court, in fact, noted that the investigation was shoddy and the investigating agency “tried to give benefit to the accused”, but did not do anything further. The accused was acquitted of all charges.

2. In the case of State by Sampigehalli Police Station, Bengaluru v. Faiz Ahamed, the accused was charged with taking intimate photographs of the victim/survivor who was unconscious at the time after consuming a spiked drink. The accused subsequently asked to marry the survivor. When her father refused, the accused threatened the father and sent him a naked photograph of his daughter. The electronic evidence was provided through CDs, copies of emails, color photocopies of the photographs, and printouts. The trial court noted the absence of the Section 65B(4) certificate for secondary evidence of this nature and dismissed the evidence as per the Anvar ruling. The accused was acquitted in this case.

These examples show that a procedural issue related to a certificate on digital evidence caused the cases to be decided differently and indicates a key concern in the delivery of justice. “The production of secondary electronic evidence in courts of law should not be prohibitively difficult for victims/survivors of technology-mediated VAW (violence against women).” The Section 65B(4) certificate has been mandated to ensure the authenticity of the document provided, but it can hinder the process of the
trial altogether. This requires course correction, which the Khotkar decision has done, to some extent, by focusing on the court’s power to summon evidence and the certificate to arrive at a just decision.

3.3.1.3 Cases where digital evidence was not considered

In a few cases, despite the presence of electronic evidence, the court did not consider it. This approach is harmful in cases of OGBV, since the site of the offense is more easily accessible in them. When such evidence is ignored, it does not serve the purpose of justice.

The complaint in State v. Narender Singh\textsuperscript{138} was about criminal intimidation and sending an “obscene message” and uploading “obscene content” on the victim’s/survivor’s profile. However, the court did not refer to any of these in its order and acquitted the accused. This could also be partially attributed to the prosecution failing to include them in the evidence. The prosecution only had four witnesses—two public witnesses, an aid to the investigating officer, and the duty officer. Even the victim/survivor was not examined by the prosecution.

When the prosecution is unable to help the courts with the necessary evidence and the courts only act in their role as a neutral arbiter rather than asking for requisite evidence for effective adjudication, it ends in a travesty of justice.

3.3.2 With advances in technology, courts must grapple with the definition of primary and secondary digital evidence in OGBV cases

A significant question in a highly digital world is: What constitutes primary and secondary evidence in the case of electronic evidence? Seemingly, the answer is straightforward: If one can produce the original laptop or mobile, it is primary evidence. However, printouts and other recordings of a computer output are secondary evidence.

The Punjab and Haryana High Court, in Rakesh Kumar Singla v. Union of India\textsuperscript{139}, refused to accept screenshots of WhatsApp messages without the Section 65B certificate. This raises some interesting questions that courts may have to grapple with in the coming years.

1. Would having the mobile phone where the WhatsApp number is active be primary evidence?
2. Would using WhatsApp Web to access messages from any laptop make it primary evidence?
3. What happens if a deep fake of a woman in India is created in one location outside the territory of India, bounced off several servers, and is accessible on the internet across multiple jurisdictions? Would all versions of the deep fake be considered primary evidence if shown on a computer, which is not the original computer? How should such evidence be classified?

The Supreme Court, in the Khotkar verdict, directed the framing of rules for retention of data in trial cases and for preservation, retrieval, and production of electronic records under Section 67C\textsuperscript{140} of the IT
Act. These have not been done yet. A review of Section 65B of the IEA has also been recommended in the Khotkar verdict.

As discussed earlier, the new draft law on evidence may alleviate some of these concerns, especially the ones around primary and secondary evidence for electronic evidence. However, until such time the law is passed, it is important to consider the concerns under the old law, which will continue to govern many cases for the next few years.

3.3.3 Courts need to revisit how to impose bail orders that acknowledge the online public sphere as well as the use of technology in OGBV cases

Legally, bail means the procurement of release from prison for a person awaiting trial or an appeal, by depositing a security to ensure his submission at the required time before a legal authority. The CrPC has categorized legal offenses as bailable and non-bailable. Most of the offenses under the IPC that are applied in cases of OGBV are bailable in nature with the exception of Section 354 (assault or criminal force against a woman with the intent to outrage her modesty), which is commonly applied in cases of sexual harassment.

Our sample mostly included criminal cases, which went on to the appeal stage to the high courts as regular or anticipatory bail applications. The common underlying trend we noticed included the receptive structures of bail conditions that were granted to the accused and the nature of reasonings provided for bail applications to justify them. One prominent observation was the sexist and patriarchal reasonings given by the courts to grant bail as well as the bizarre conditions imposed on the accused while granting such bail. The sexism or judicial stereotyping in the bail reasoning was obvious through their focus on the character of the complainant as opposed to the behavior of the accused or a description of the offense committed. These trends have been captured in the cases mentioned in Table 4. These cases indicate the pervasive sexism within bail orders and the way a procedural function like bail has also been clouded by biases, which often leads to a miscarriage of justice for the victim/survivor.

Table 4 mentions the reasons and conditions given by courts across various bail orders. Some were based on universal standards and principles while granting bail while others were cases where courts placed bizarre conditions based on manifestly patriarchal or sexist reasonings.
In the two cases mentioned below, the judges have made remarks referring to the accused men—both of whom, as per the facts of the case, are 23 and 21 years of age—as “young boys”. Under the CrPC, a person accused of an offense is entitled to be released on bail pending trial unless there are reasonable grounds to believe that they are likely to abscond, tamper with evidence, or interfere with the investigation or prosecution of the case. In determining whether to grant bail, courts in India consider a variety of factors, including the seriousness of the offense, the nature of the evidence, the likelihood of conviction, the accused’s criminal record, and the potential danger posed to society by the accused. It is common practice for the court to account for the individual circumstances of the accused, such as their age, health, and family situation. This is common across the cases as the right to bail is equally available to all citizens and the court grants bail while striking a balance between the need for the accused to be brought to justice and the principle of presumption of innocence until proven guilty. However, referring to an adult man as a “young boy” can undermine his agency and responsibility as an adult, and can perpetuate harmful stereotypes about masculinity and maturity. The point to note is about the court practice as opposed to the process of granting bail. It is important to use appropriate and respectful language when referring to individuals in judgments and orders, regardless of their age or gender. “Young boys” or “boys” are those below the age of 18 and have a separate legislation to address juvenile crimes. However, in the cases below, the charges were all based on the IPC or IT Act and were not to be treated as offenses by a child or young adult. Notably, an explicit mention of the term “young boy” became a part of the order/judgment while granting bail.
<table>
<thead>
<tr>
<th>Case name and brief facts</th>
<th>Bail status</th>
<th>Bail conditions(^{144})</th>
<th>Excerpts of reasons for granting bail(^{145})</th>
</tr>
</thead>
</table>
| **Chhotelal v. The State of Madhya Pradesh\(^{146}\)** | Granted | 1. Applicant to furnish a personal bond of ₹30,000.  
2. The applicant shall abide by the conditions as enumerated under Section 437(3) of the CrPC. | “On going through the case diary, it seems that there is no criminal antecedents of the applicant. The applicant is a young boy of 23 years and is in judicial custody since 26.12.2018.” |
| The applicant allegedly took the prosecutrix’s mobile phone, removed the memory card, and did not return it on her request. Later, he made a fake Facebook account and uploaded objectionable photographs of the prosecutrix on that account, leaving it open so that the public could view the photographs. The case of the applicant was that he had been falsely implicated and had been in custody for two weeks. | | | |
| **Vikash Rajak v. The State of Madhya Pradesh\(^{147}\)** | Granted | 1. Bail bond of ₹100,000.  
2. The applicant will cooperate in the trial.  
3. He will not indulge himself in extending inducement, threat, or promise to any person acquainted with the fact of the case to dissuade him from disclosing such facts to the court or to the police officers.  
4. He will not commit any similar offense.  
5. He will not seek unnecessary adjournments during the trial.  
6. He will not leave India without previous permission of the court in view of the outbreak of Covid-19, the applicant shall also comply with the rules and norms of social distancing. | “Applicant is young boy aged 21 years and if he will remain in custody, then the future of his family will become spoiled.” |
Factors like age and marital status impact sexual victimization, with younger, unmarried, or separated women being at higher risk. In fact, studies show that typical rape victim/survivor that the courts generally believe are likely to be sexually inexperienced people who lead ‘respectable lifestyles’. This creates scope for a situation where older women, especially those who are married, are considered less likely to be victims/survivors of sexual offenses. Additionally, marriage exerts control over a woman’s sexuality. In India, it leads to expectations of the way a married woman ‘should’ behave, including seeking permission from family elders to step outside her home, gender segregation, and control over economic resources. Violating these inherent societal codes of behavior can earn social reprisal. While analyzing the cases from our sample set, we noticed that the courts often noted the marital status or occupation of the woman without providing any specific reason for doing so. Contextually, these statements were not placed along with the facts of the case. In the cases below, some even go onto the extent of characterizing the woman’s response during the assault, as not the way, “our women react when they are ravished” and taking note of the fact of them not “informing the police”.

Typical reactions in cases of sexual violence are based on stereotypes and myths. The Supreme Court, in *Aparna Bhat v. State of Madhya Pradesh*, identified the following gendered stereotypes that courts should avoid using: “(i) women are physically weak and need protection; (ii) women are incapable of or cannot take decisions on their own; (iii) men are the ‘head’ of the household and should take all the decisions relating to family; (iv) women should be submissive and obedient according to our culture; (v) ‘good’ women are sexually chaste; (vi) motherhood is the duty and role of every woman, and assumptions to the effect that she wants to be a mother; (vii) women should be the ones in charge of their children, their upbringing and care; (viii) being alone at night or wearing certain clothes make women responsible for being attacked; (ix) a woman consuming alcohol, smoking, etc., may justify unwelcome advances by men or ‘has asked for it’; (x) women are emotional and often overreact or dramatize events, hence it is necessary to corroborate their testimony; (xi) testimonial evidence provided by women who are sexually active may be suspected when assessing ‘consent’ in sexual offense cases; and (xii) lack of evidence of physical harm in sexual offense case leads to an inference of consent by the woman.” While this list is not exhaustive of all types of stereotypes, it provides a clear view of the kinds of gendered notions that persist in society and in courtrooms.

Both victim/survivor blaming and gender role-based judgments are harmful and can lead to unfair and unjust outcomes in legal proceedings. They can perpetuate harmful stereotypes and contribute to a culture of victimization and oppression. The focus must be on the evidence and facts of the case rather than stereotypes or assumptions about the behavior or character of the victim/survivor or perpetrator based on their gender or other personal characteristics.
Table 5. Some gendered stereotypes that persist in society and in courtrooms

<table>
<thead>
<tr>
<th>Case name and brief facts</th>
<th>Bail status</th>
<th>Bail conditions&lt;sup&gt;154&lt;/sup&gt;</th>
<th>Excerpts of reasons for granting bail&lt;sup&gt;155&lt;/sup&gt;</th>
</tr>
</thead>
</table>
| **Anand Mohan v. The State of Bihar**<sup>156</sup>  
The informant is a married lady and has two children. She had developed a friendship with the petitioner about three years ago through Facebook. On 12 March 2019, the petitioner called her on the eve of the marriage of his sister. At about 11:00 p.m., the petitioner gave a cold drink to the informant and after consuming it, she became unconscious. Thereafter, the petitioner and his brother-in-law established physical relations with her and video recorded it. She further alleged that Anand Mohan blackmailed her and extracted ₹500,000 from her. They also threatened to kill her and her children. The petitioner alleged that they had been in a consensual relationship. The informant filed a case for rape after more than one year only to extract money from the petitioner and pressurized him to marry her.| Granted | 1. Bail bond of ₹10,000.  
2. Compliance with conditions as laid down under Section 438(2) of the CrPC. | “Having considered the submissions of both sides and on perusal of the F.I.R. as well as the case-diary, it appears that the **victim, who is a married woman, developed [a] friendship with the petitioner […] on whose request, she went to the house of the petitioner on the eve of [the] marriage of his sister but she alleged that on 12.03.2019 the petitioner along with his brother-in-law forcibly established physical relation with her. **Even on the next day, the informant (prosecutrix) did not inform the police. She kept mum and allowed the petitioner to have physical relations for more than a year.** Thereafter the victim filed the case. On the face of it, it appears that the victim, who is a major married lady, had consensual sex with the petitioner although the petitioner denied the allegation.**”<sup>157</sup> |
**Case name and brief facts**

*Bri Rakesh B v. State of Karnataka, 2020*

The complainant has alleged that she was subjected to rape on the false promise of marriage.

<table>
<thead>
<tr>
<th>Bail status</th>
<th>Bail conditions</th>
<th>Excerpts of reasons for granting bail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Granted</td>
<td>1. Bail bond of ₹100,000. 2. Petitioner shall cooperate in the investigation/further investigation at all times and appear before the jurisdictional police, if and when, so directed; 3. He shall not leave the jurisdictional limits of the trial Court without its prior permission; 4. He shall mark his attendance in the jurisdictional Police Station every second and fourth Saturday of the calendar month between 9.00 am and 3.00 pm; 5. He shall not tamper the evidence or influence/deter the witnesses/victims; nor shall he do anything prejudicial to peace &amp; order in the civil society; 6. It is open to the jurisdictional police or the complainant to seek cancellation of bail if and when the petitioner commits breach of any of the above conditions or perpetrates any offense hereafter.</td>
<td>“The Court finds it hard to believe the complainant’s allegation of rape given there is a letter allegedly written by the complainant to the effect that she was ready to withdraw the complaint if a compromise is brought about, especially when the complainant had employed the services of the petitioner for the last two years or so. She should have come to the court when the petitioner was allegedly forcing her for sexual favours.” The Court has also questioned why she went to her office at night, i.e., 11.00 p.m.; “she has also not objected to consuming drinks with the petitioner and allowing him to stay with her till morning; the explanation offered by the complainant that after the perpetration of the act she was tired and fell asleep, is unbecoming of an Indian woman; that is not the way our women react when they are ravished.” Such statements perpetuate harmful stereotypes about how women “should” behave in response to sexual assault and rape, and it is not based on any factual or legal basis. A victim of sexual assault or rape may have various reasons for not immediately reporting the crime, including fear, shame, and social stigma. The fact that the victim may have consumed drinks or allowed the accused to stay with her until morning does not imply that she consented to sexual activity or that the assault did not occur. Further, it is not appropriate to make generalized statements about how “Indian women” should or should not react to sexual assault or rape. Each individual reacts differently to traumatic experiences, and there is no one “correct” or “expected” way that victims should behave. In recent years, there has been a growing recognition in India of the harmful impact of victim-blaming and gender stereotypes in sexual assault and rape cases. Courts have become more sensitive to the experiences of victims and have adopted a more victim-centric approach to adjudicating such cases, but still need to keep the same in mind even when online crimes are involved.</td>
</tr>
</tbody>
</table>
It is important to note that across the cases selected for this study, when it comes to the question of bail, there are two aspects that must be revisited keeping in mind the changing and viral nature of online violence. First, reasonings for bail orders, which still tend to be patriarchal, must be based on law and evidence and, second, bail conditions, which currently do not reflect the online public sphere and still follow a standard template of principles, must change overtime. The following sections are deep-dives into these two points.

3.3.3.1 Reasonings for bail orders

Unlike the magistrate’s court, which has limited powers for granting bail, high courts have broad powers and can grant bail for all offenses. In Rao Harnarain Singh v. State of Punjab, it was observed that courts have to consider several factors while granting bail, including the enormity of the charge, the nature of the accusation, the severity of the punishment that the conviction will entail, the nature of evidence supporting the accusation, the dangers of the applicant absconding if released on bail and of the witnesses being tampered, the protracted nature of the trial, the opportunity for the applicant to prepare for his defense and access to a lawyer, and the health, age, and sex of the accused.

The Supreme Court, in Gudikanti Narasimhulu v. Public Prosecutor, also held that the previous criminal history of an accused must be factored in while granting bail. While granting bail, the court also imposes certain conditions on the accused, which are to be complied with, and their violation can result in the bail being cancelled.

The immense discretion of the courts in granting or denying bail to an accused in cases of non-bailable offenses comes at a cost. The usual bail order looks like a facsimile of the same manuscript enlisting a few platitudinous conditions. But every once in a while, a bail order is passed containing some bizarre bail conditions. In July 2020, in the case of Vikram v. State of Madhya Pradesh, a bail order caused quite a furor when the Madhya Pradesh High Court ordered the accused to get a rakhi tied by the complainant as a bail condition. Almost a year later, in the Aparna Bhat verdict, the Supreme Court set aside the paternalistic and manifestly sexist order while also issuing a set of guidelines for courts to follow while dealing with sexual crimes:

“(a) Bail conditions should not mandate, require or permit contact between the accused and the victim. Such conditions should seek to protect the complainant from any further harassment by the accused;

(b) Where circumstances exist for the court to believe that there might be a potential threat of harassment of the victim, or upon apprehension expressed, after calling for reports from the police, the nature of protection shall be separately considered and appropriate order made, in addition to a direction to the accused not to make any contact with the victim;
(c) In all cases where bail is granted, the complainant should immediately be informed that the accused has been granted bail and copy of the bail order made over to him/her within two days;

(d) Bail conditions and orders should avoid reflecting stereotypical or patriarchal notions about women and their place in society, and must strictly be in accordance with the requirements of the CrPC. In other words, discussion about the dress, behavior, or past ‘conduct’ or ‘morals’ of the prosecutrix, should not enter the verdict granting bail;

(e) The courts while adjudicating cases involving gender related crimes, should not suggest or entertain any notions (or encourage any steps) towards compromises between the prosecutrix and the accused to get married, suggest or mandate mediation between the accused and the survivor, or any form of compromise as it is beyond their powers and jurisdiction;

(f) Sensitivity should be displayed at all times by judges, who should ensure that there is no traumatization of the prosecutrix, during the proceedings, or anything said during the arguments, and

(g) Judges especially should not use any words, spoken or written, that would undermine or shake the confidence of the survivor in the fairness or impartiality of the court.”

The guidelines listed above make it abundantly clear that there are several extraneous considerations for the courts while hearing bail applications, both regular and anticipatory. In Sajeev v. State of Kerala167 as well as in the Anand Mohan verdict, the marital status of the woman played a significant role in granting bail. As such, controlling women through the institution of marriage is deeply ingrained in society and is often reflected in courtrooms as well.168 In Sri Rakesh B v. State of Karnataka,169 the court questioned the conduct of an Indian woman by stating that:

“She has also not objected to consuming drinks with the petitioner and allowing him to stay with her till morning; the explanation offered by the complainant that after the perpetration of the act she was tired and fell asleep, is unbecoming of an Indian woman; that is not the way our women react when they are ravished.”

This kind of judicial stereotyping of women in adjudication of cases is exactly what the Aparna Bhat case aimed to address. It cautioned against:

“The use of reasoning/language which diminishes the offense and tends to trivialize the survivor, is especially to be avoided under all circumstances. Thus, the following conduct, actions or situations are hereby deemed irrelevant, e.g., to say that the survivor had in the past consented to such or similar acts or that she behaved promiscuously, or by her acts or clothing, provoked the alleged action of the accused, that she behaved in a manner unbecoming of chaste or ‘Indian’ women, or that she had called upon the situation by her
behavior, etc. These instances are only illustrations of an attitude which should never enter judicial verdicts or orders or be considered relevant while making a judicial decision; they cannot be reasons for granting bail or other such relief.”

3.3.3.2 Conditions for bail

Keeping in mind cases of OGBV, the discourse around the manner of imposing bail conditions needs to be revisited. Through the cases in our sample, we noticed the general trend of conditions being repeatedly used, not accounting for the online public sphere and the role of technology in mediating violence. Some of these general conditions include:\textsuperscript{170}

1. Abiding by specified restrictions on personal associations, place of abode, or travel;
2. avoiding all contact with an alleged victim/survivor of the crime and with a potential witness who may testify concerning the offense;
3. regularly reporting to a designated law enforcement agency;
4. refraining from possessing and surrendering if in possession of any firearm, ammunition, destructive device, or other dangerous weapon;
5. undergoing available medical, psychological, or psychiatric treatment, and remaining in a specified institution, if required, for that purpose;
6. satisfying any other condition that is reasonably necessary to secure the appearance of the person, as required, and to ensure the safety of any other person and the community;
7. surrendering the passport or any other travel document in the possession of the accused; in case the accused does not have one, he may be prohibited from obtaining one;
8. seeking or maintaining employment or entering into any educational program;
9. refraining from attending such premises or any other place as the court may specify;
10. abiding by any restriction on travel or movement; or
11. abiding by specific restrictions on speech and expression.

Some of these generalized conditions, such as “avoiding all contact with an alleged victim/survivor of the crime”, could be interpreted to include contact online means in the online public sphere. However, bail conditions directly related to the usage of online tools, with specific emphasis on online activities, must be implemented. For instance, in the case of \textit{R v. Bower},\textsuperscript{171} in the United Kingdom and in a cyberstalking case in Canada called \textit{R v. Morrison},\textsuperscript{172} the accused was granted bail but was required to surrender his passport, stay away from the victim/survivor, and avoid using any electronic device to communicate with the victim/survivor or any of her family members.
None of the cases in our study had any peculiar condition pertaining to the internet, social media platforms, or technology/communication devices. Bail orders do not seem to have been customized to the unique requirements of cases of OGBV yet.

This is not to say that courts are not cognizant of the use of social media or restricting it, especially when the cases are of a political nature. Courts have often been highly creative with bail orders in cases that do not have an aspect of gendered violence. The Madras High Court, in 2019, in Jabin Charles v. State of Tamil Nadu, while granting anticipatory bail to a Tamil Nadu resident who had been booked for an alleged derogatory Facebook post against the Indian Prime Minister, imposed a condition of staying away from social media for a year. However, this move was criticized as a violation of citizens’ fundamental right to free speech.

Such peculiar bail orders are not unique to India. Jimmy Lai, one of Hong Kong’s most vociferous anti-government voices, was charged under China’s new law to quell protests in December 2020. Later in the month, a Hong Kong judge granted the media tycoon bail but only after imposing extensive restrictions barring him from using social media, giving interviews, or leaving his home, evoking concerns of deterioration of free speech.

Similarly, the Madhya Pradesh High Court came up with several peculiar bail orders over the course of the pandemic. In Arvind Patel v. State of Madhya Pradesh, as a pre-condition for bail, it directed the two accused to install colored LED televisions, manufactured anywhere but in China, at a local district hospital. The court ordered the accused in the case of Badal Singh & Ors. v. State of MP & Anr to register as a Covid warrior, and to donate masks and sanitizers in Jujhar v. The State Of Madhya Pradesh.

While imposing conditions in bail orders, courts must ensure that the conditions align with the offense, with the attendance of the accused during trial, or with the trial being conducted fairly. In the case of Narasimhulu v. Public Prosecutor, Justice Krishna Iyer iterated that:

“It is imperative that discretion must be exercised with caution and care and must be applied by balancing the interests of both justice and personal liberty of individuals. It must not be arbitrary, vague, and fanciful, but legal and regular. Conditions may be hung around bail orders, not to cripple but to protect.”

The Aparna Bhat verdict highlights how bail conditions that tend to condone or diminish the harm caused by the accused can potentially expose the victim/survivor to secondary trauma. Such bail conditions include mandating mediation processes in non-compoundable offenses, mandating community service, requiring an apology to be tendered to the victim/survivor once or repeatedly, and getting or staying in touch with the victim/survivor in any manner. The bail order should not permit any
conduct where the victim/survivor may be retraumatized or be led into some kind of involuntary acceptance, and it should not allow the behavior of the accused to be condoned in any way.

In *Jameel Ahmad v. Mohammed Umair Mohammad Haroon & Anr*,[180] the Supreme Court stated that although granting bail is a discretionary order, courts must exercise this discretion judiciously while applying certain settled parameters. The overarching powers granted under Section 437(3) of the CrPC to impose “any condition” must not be interpreted literally as conferring absolute power on a court of law to impose any condition that it chooses to impose. In *Joginder Kumar v. State of UP*,[181] the court observed that the condition must be in consonance with the object and purpose of granting bail, and any condition not having an iota of nexus with the very objective of granting bail cannot be imposed.

### 3.3.4 Role of courts

Courts need to revisit the way to impose bail conditions in light of acknowledging the online public sphere as well as the use of technology while keeping in mind the principles of fair bail conditions that do not violate fundamental rights. We were unable to find any definitive patterns in our sample case where the courts tried to do this, thus highlighting the gap in the acknowledgment of online crimes at the stage of bail hearings.

To quote a high court verdict, “Law should not sit limply, while those who defy it go free and those who seek its protection lose hope.”[182] Criminal law and the criminal justice system must not let individuals’ right to personal liberty be invaded by others, and they must protect the weak against the powerful and the influential. To this end, the State prescribes rules of conduct, sanctions for violations, machinery to enforce them, and procedures to protect the machinery,[183] but what happens when biases start influencing the world of criminal justice?

Many women and marginalized groups hesitate to file complaints due to apprehension of injustice, hesitancy in filing complaints,[184] and the stigma, sexism, and misogyny one has to face when approaching the courts.[185]

To summarize, in the cases of OGBV that we analyzed, we noticed two important reasons for the miscarriage of justice: first, not filing the procedural Section 65B certificates for electronic evidence, and, second, making sexist remarks about the victim/survivor to grant bail to the accused.

As we delve deeper into our analysis, it becomes evident that while challenges persist in OGBV cases, there is also a notable shift in judicial approaches. This shift is reflected in the emerging jurisprudence on social media governance in India, which forms the core of our next finding. Exploring this evolving legal landscape, we aim to uncover how courts are increasingly attempting to hold online platforms accountable in the context of OGBV cases, thereby shaping the trajectory of digital justice.
3.4 Finding 4: Courts are attempting to hold platforms accountable in OGBV cases, leading to emerging jurisprudence on social media governance in India

“The technological age has produced digital platforms – not like the railway platforms where trains were regulated on arrival and departure. These digital platforms can be imminently uncontrollable at times and carry their own challenges. One form of digital platforms are the intermediaries that claim to be providing a platform for exchange of ideas without any contribution of their own. It is their say that they are not responsible for all that transpires on their platform; though on complaints being made, they do remove offensive content based on their internal guidelines. The power and potentiality of these intermediaries is vast, running across borders. These are multinational corporations with large wealth and influence at their command. By the very reason of the platform they provide, their influence extends over populations across borders. Facebook is one such corporation.”

-Ajit Mohan v. Legislative Assembly, NCT & Ors. (8 July 2021).

The escalation of online violence based on gender is a global phenomenon that has been growing by the day. The supposedly neutral social media platforms have been a breeding ground for violence for years. Evidence of companies like Facebook, Twitter/X, and YouTube hosting and fostering violence, including the circulation of rape videos and revenge porn have existed since as early as 2014.186 Women who have come out in the public sphere to recount their experiences have only been targeted more. A few examples have been listed below.

1. Thorlaug Agustsdottir reported a Facebook group that shared pictures of beaten/chained women in general, in addition to a morphed and bruised image of her face with comments like, “Women are like grass, they need to be beaten/cut regularly.”187

2. Anita Sarkeesian received overwhelming hate, including virtual game bludgeoning, for developing a feminist YouTube series.188

3. Sagarika Ghose, an activist, is regularly threatened—with gang rape and being stripped—on Twitter/X for her anti-right wing, “sickular” views.189

4. Meena Kandasamy, a Dalit poet and activist, faced threats of live-streamed gang rape, immolation, and acid attacks after she posted about her participation in a beef-eating festival in Kerala, India on Twitter/X.190

Studies by IT for Change,191 BBC Panorama,192 Equality Labs,193 and Amnesty International194 have shown that women in public life face more violence on social media platforms. Courts play a big role in
acknowledging how such platforms foster violence, and what pivotal steps need to be taken to effectively remove harmful content.

Social media platforms famously profit immensely from high user engagement on content. It has also been documented that the virality of hateful content is also a profiteering mechanism. In India, where Facebook has the largest market share of users, the virality of hate as a tool to increase engagement has been seen through an incident that became widely popular. When Kapil Mishra, an Indian politician, incited violence through his Facebook page, causing riots in New Delhi, the interactions on his Facebook page, “grew from a couple hundred thousand interactions a month to more than 2.5 million”. Even more shocking were the UN’s revelations that Facebook had been a major platform for spreading hatred against the Rohingyas in Myanmar, which led to the ethnic cleansing of the community in the region.

Courts have the power to acknowledge and address these deliberate choices made by social media platforms to further harmful content for the sake of virality. The adverse impact that OGBV has on victims/survivors and society at large was recognized by the Kerala High Court in *P. Sreekumar v. State of Kerala* in 2019, echoed in *Sreeja Prasad v. State of Kerala* in May 2020. In the latter, the court noted the increasing intolerance and othering in social media discourse with concern. In July 2021, in *Ajit Mohan v. Legislative Assembly*, the Supreme Court recognized that for social media platforms in the modern technological age, the defense of being neutral conduits and mere platforms for an exchange of ideas is not tenable, given their business models. The court highlighted:

1. The concerns expressed globally by governments, including the need for greater accountability by intermediaries that can influence millions of people;
2. how independent democracies are leading movements to ensure that these mediums do not become tools of manipulative power structures; and
3. how platforms are, by no means, altruistic in nature but rather employ business models that can be highly intrusive of individuals’ privacy and potentially polarize public debates.

In fact, Facebook itself acknowledged that it removed 22.5 million pieces of hate speech content in the second quarter of 2020 (up from just 1.6 million pieces of hate speech removed in the last quarter of 2017), nearly 95% of which we removed before it was reported to Facebook - reflecting their substantial degree of control over the disseminated/online content.

In this context, this section attempts to understand how social media is used and acknowledged in the courts. We argue that it is important to hold big, global, highly influential social media entities and intermediaries accountable for their duty to care for their users and move beyond safe harbor arguments.
It is equally, if not more, important for the Indian judicial machinery to exercise its powers to:

1. Observe critical aspects of online violence arising out of the cases that are placed before them;
2. devise effective ways to tackle further violence; and
3. add to and update Indian cyber law jurisprudence.

3.4.1 Courts have to grapple with a myriad of online offenses perpetrated on social media, including NCIID and gender trolling

From our research, the violence perpetrated in the online public sphere covered a range of offenses. Some of these cases have been listed below as examples.

1. In *Kishore K Swamy v. State*, the accused, in addition to cyberstalking the victim/survivor, posted abusive messages on her Twitter/X and Facebook with the intention of defaming her.203

2. In *The Present Petition Has Been v. Unknown*, the accused made obscene comments and posts about several women through his Twitter/X and Facebook profiles.204

3. In *X v. Union of India and Ors*, photographs and images that a woman had posted on her private social media accounts on Facebook and Instagram were taken without her knowledge or consent and unlawfully posted on a pornographic website by an unknown entity called Desi Collector. In this case, the petitioner’s photographs became offensive by association.205

4. In *X v. YouTube*, a prominent Indian actor, initially promised a lead role in a web series by Ram Gopal Verma Studios, faced distress when explicit scenes from the shelved project were shared online by the producer and unauthorized individuals. This was done without the consent of the plaintiff. Some of the videos were superimposed with objectionable commentary on the videos. The plaintiff was trolled after.206

5. In *Bijo v. State of Kerala*, the accused posted a pornographic video of a naked woman on a WhatsApp group.207

From our sample set of cases, some of the recurring offenses mediated via social media include:

1. NCIID resulting in image-based sexual abuse;
2. posting private photos online;
3. uploading images to pornographic websites;
4. illegal recordings and uploading of such pictures, images, or videos;
5. creating fake accounts;
6. intimidation and extortion, and
3.4.1.1 What are the common platforms being used based on our sample of cases?

From our sample study, a majority of cases were primarily based on offenses committed on Facebook, Twitter/X, and WhatsApp. However, we also found cases where violence was perpetrated on Instagram, YouTube as well as other platforms, like specific websites being created for NCIID, or pornographic websites, to name a few.

3.4.2 Courts are attempting to hold platform intermediaries responsible for promptly taking down violent content in OGBV cases

In The Present Petition Has Been ... v. Unknown, a bail appeal for a case of gender trolling, the petitioner spread fake and scandalous news against women (most of them belonging to the media) using his Facebook and Twitter/X accounts. In this context, in 2020, the Madras High Court recognized:

1. The nature of the posts (including vernacular derogatory posts) and the social media accounts they are being posted on (Facebook and Twitter/X);
2. how, even today, women are not given the requisite space online to express themselves, which is a constitutional guarantee for all Indians based on the right to equality; and
3. the disregard that the accused displayed for women, including his “crooked and vulgar mind”, while posting the tweets.

In our sample set of cases, we observed that only a few cases actively acknowledged the nature of online offenses on social media platforms as harmful or as a concern. Further, regarding cases that involved violence on online intermediaries, very few recognized the role of social media platforms or the relevant intermediaries and requested their involvement in taking down offensive content. Two cases that recognized social media governance issues as well as the challenges faced by courts in working with intermediaries have been highlighted in the following sections.

3.4.2.1 Inability to completely remove violent content

In a 2021 case before the Delhi High Court, X v. Union of India and Ors, the social media accounts of the petitioner, despite having the requisite ‘privacy settings’, were compromised, and her photographs and images were taken and posted on a pornographic website. One of the key aspects of this case is the issue of cross-functioning between the court, intermediaries, and the State (investigation authorities like the police). The arguments provided by each entity highlight the challenges of enforcement.

The Delhi Police highlighted how social media platforms, instant messaging services, e-mail services etc., instead of responding expeditiously to their requests for information, sometimes ask law
enforcement agencies to produce letters rogatory (LRs) and resort to prolix remedies under mutual legal assistance treaties (MLATs), even when unlawful content has been uploaded from an Indian IP address. The Delhi Police emphasized how this causes much delay in obtaining the necessary information and material to book the accused, who continue to repeatedly upload unlawful content, as seen in *X v. Union of India and Ors*.

On the other hand, intermediaries highlighted how, when it comes to the issue of removal of content or blocking access, the role of the search engine is “reactive”, not “proactive”. It is limited to disabling access to specific URLs by removing them from the search results once they have been reported by governmental agencies or ordered to be pulled down by the courts. Reinforcing the safe harbor argument, the platforms emphasized how search engines cannot be tasked with adjudicating the legitimacy of the content searched through them. The limitations in taking down content in this particular case were highlighted by the intermediary stating that image-based search results, unlike text-based results, are more difficult to identify and retrieve. This is because an image search employs complex algorithms that use information about an image, such as the name of the image file as stored on a web page, information about the web page on which the image appears, and other similar information. They also submitted how technological and automated means would not be able to differentiate or exercise any discretion regarding the content uploaded on the platforms, particularly when content is unlawful due to its context.

Through the course of hearings, the court noted some key points in its order.

1. **Regarding the perpetrators**: The court noted that it cannot permit itself to resign to the cat and mouse game of errant parties evading court orders by reposting offending content across the internet, in an act of defiance and contumacy.

2. **Regarding the state**: The Cyber Prevention Awareness and Detection Unit (CyPAD)\(^{210}\) expressed their willingness to obey the court orders to remove or disable offending content, but they also expressed their inability to fully and effectively remove it in compliance with court directions.

3. **Regarding the intermediaries**: The court observed that for the removal or disablement of offending content to be effective even within India, a search engine must block the search results throughout the world, since no purpose would be served by issuing such an order if it has no realistic prospect of preventing irreparable harm to a litigant. The court acknowledged the difficulties expressed by the intermediaries but also highlighted that an intermediary cannot be heard saying that it is unable to remove or disable access to offending content despite such actual knowledge as contemplated in law.
4. **Regarding the role of the court:** The issue of removing offending content is equally, if not more, significant at the time of interim orders when a case is taken up by the court. If the court is not in a position to pass effective and implementable orders, and is unable to ensure that such orders are complied with at the interim stage, subsequent adjudication of the matter could be rendered infructuous.

Thus, the court acknowledged its own role in giving effective content takedown orders and went a step ahead to institute specific and pointed instructions to the parties in the case. The court emphasized that even if the offending content cannot be completely removed from the internet, it can be made unavailable and inaccessible by making it “non-searchable”. This would involve de-indexing and de-referencing such content from the search results of the most widely used search engines. In this context, the court issued directions to the following stakeholders.

1. **Search engines:** The search engines Google Search, Yahoo Search, Microsoft Bing, and DuckDuckGo, were directed to globally de-index and de-reference the offending content as identified by its web and image URLs, from their search results. This included de-indexing and de-referencing all concerned web pages, sub-pages or sub-directories on which the offending content would be found within 24 hours of receipt of the judgment.

2. **Police:** The Delhi Police were directed to obtain all information and associated records relating to the offending content such from the concerned website, namely www.xhamster.com, and from the search engines, Google Search, Yahoo Search, Microsoft Bing, DuckDuckGo (and any other search engines as may be possible). This included the URL, account ID, handle name, IP address, hash value, and other such information as may be necessary for the investigation of a case within 72 hours of receipt of the judgment.

The court consciously noted that even though no untenable burden should be cast upon an intermediary, they must comply with the order. The court also pertinently highlighted the consequences of non-compliance of such orders:

1. Forfeiting the safe harbor exemption available to intermediaries under Section 79(1) of the IT Act and as specified by Rule 7 of the 2021 Rules; and
2. holding an intermediary entity and its officers liable for action as mandated by Section 85 of the IT Act.

It is essential to have a proper and efficient mechanism to implement a content takedown order. In courtrooms, when intermediaries use the defense of a “lack of technical ability” to remove content, the same cannot be encouraged. As seen in this case, the court appointed an *amicus curiae* to come up with the most effective solution in tackling content takedown issues. The objective of the court should
be to ensure that there is no restriction on the freedom of speech and expression, which is a constitutional right guaranteed to every gender identity. These issues, including content takedowns, must be juxtaposed with the rights guaranteed to individuals. The courts must carve out relevant jurisprudence and effective orders to ensure an online public sphere without violence or hate speech. Further, the courts should note the displacement of marginalized voices from the online public sphere due to violence as a violation of various fundamental rights. Courts have the inherent power to identify such rights, discuss possible solutions, and come up with effective and clearly defined orders.

3.4.2.2 Safe harbor arguments in courtrooms

In *Sasikala Pushpa v. Facebook India*, the plaintiff alleged that the circulation of her photograph—through social media platforms like Facebook, Twitter/X, YouTube, and WhatsApp—with a man from a rival political party was defamatory. The plaintiff argued that allowing further publicity to such a photograph/video would only serve sensational and salacious purposes, and it would amount to a gross and irreparable violation of an individual’s privacy—it would be defamatory per se. While the case was later purely adjudicated as an issue of whether the content was defamatory, it is imperative to see the arguments put forth by Facebook India in this context. Facebook had filed a written statement in the case pleading the following points.

1. Facebook is an intermediary, as defined under Section 2(1)(w) of the IT Act, and is omitted from any liability arising from third-party content posted to the Facebook Services as per Section 79 of the IT Act.

2. Section 79(1) of the IT Act has an overriding effect by virtue of Section 81 of the IT Act.

3. As an intermediary, Facebook Inc. has no role in sharing, transmitting, and selecting the receiver of any transmission, and/or selecting or modifying the information contained in any information of a third party.

4. There is no averment in the plaint regarding any failure of Facebook Inc. to comply with Section 79(2) or 79(3) of the IT Act, and it does not even allege that protection under Section 79 of the IT Act is not available to Facebook Inc.

5. As per the dicta of the Supreme Court in *Shreya Singhal v. Union of India*, the liability of an intermediary arises only where the intermediary, upon receiving actual knowledge from a valid court order or otherwise that unlawful acts related to Article 19(2) of the Constitution of India are going to be committed, fails to expeditiously remove or disable access to such material.

6. Facebook Inc., as of 30 June 2018, had over 2.23 billion active users of its Facebook service worldwide and every day billions of pieces of content are posted and shared on the Facebook
service; it is impractical and not possible for Facebook Inc. to sift through all the aforesaid content to find the content impugned by the plaintiff.

7. Facebook Inc. is neither the author nor the publisher of any third-party content, including the content impugned in this suit.

Mark Bartholomew, a professor of law at the University at Buffalo, noted that, "The more we think about Facebook as a business run by people with their own biases and motivations, and not simply a neutral conduit for information, the better." The basis of the safe harbor is the idea that intermediaries are dumb conduits for the distribution of their users’ speech, rather than being speakers themselves. However, this argument of intermediaries being dumb conduits is no longer tenable and should not be encouraged in courts. Most, if not all, intermediaries affirmatively shape the form and substance of user content through artificial intelligence systems and design interventions.

So, how can ‘neutral’, ‘dumb’ or any other term signify their lack of involvement? A user interface is deterministic and affects the nature and content of a platform. For example, Twitter’s/X’s 280-character limitation and some of its features, including likes, retweets, and hashtags, determine the syntax and vocabulary of the content posted on it. Thus, platforms must be held to stringent legal standards commensurate with their immensely consequential societal function. Based on our sample of cases, we submit that it is essential to recognize the virality of hate and the algorithmic amplification of such content while looking beyond the individualistic frame of the victim–perpetrator binary.

That said, platforms with multi-billion-dollar revenues are unlikely to face any issues in expending endless amounts of energy or legal power to challenge such orders. However, their users are likely to spend more resources fighting such cases in general. Further, the argument about platforms being a safe harbor for the users’ activities, under Section 79 of the IT Act, is likely to be a constant defense. This argument has been used in courts in a multitude of cases. In response, the courts have only been able to recognize the abuse of power, as they did in Ajit Mohan, by saying that relying on simplistic models such as these “would amount to shirking of their responsibilities with respect to content regulation on their site”.

Dismantling the notion of platforms as ‘dumb conduits’ that play a passive role in relaying content has been central to the perspective of our study. The power structures of social media companies must be recognized. The abuse of the judicial system in technology-related litigation is a concern. As we have seen through our case laws, Section 79 of the IT Act (India’s safe harbor provision) needs to be revisited and only courts have the power to enforce effective orders highlighting consequences of non-compliance by taking away the exemption, if required.
Impleading intermediaries and social media platforms in cases should be a “best practice” for courts, under the Code of Civil Procedure Order 1, Rule 10. This enables the court to add any person as party to the case at any stage of the proceedings, if the person’s presence before the court is necessary to enable it to effectively and completely adjudicate upon and settle all the questions involved in the case. For instance, in a public interest litigation (PIL) initiated by an NGO, Prajwala, in 2017, the Supreme Court took cognizance of the circulation of videos of rape online and made Facebook, Yahoo, Google, and Microsoft respondents to the case. This practice enables courts to help the victim/survivor more effectively to pass orders to prevent repeated violence online in cases of OGBV, like NCIID.

The governance and regulatory approaches for social media differ from country to country. Germany, for instance, requires social media companies to quickly take down “manifestly illegal” content, including hate speech, or face large fines. Australia has taken a similar approach, wherein platforms are required to quickly remove “abhorrent violent material” or face large fines. However, the US does not have such strict liability measures or increased regulations, as can be evidenced from incidents, including the Capitol Riots of 2021, which fomented on social media.

India is the world’s biggest internet-enabled nation, with over 800 million citizens online. Keeping in mind the unprecedented growth of social media users, the government, in 2021, implemented the much-debated IT Rules, 2021. The IT Rules, 2021 mandate significant social media intermediaries to enable the identification of the first originator of the information if an order is passed by the court or authority in connection with rape and sexually explicit or child abuse material. However, this responsibility reflects how the legislature views social media regulation as an individual as opposed to a collective problem. The objective of finding a sole perpetrator or originator does not address the role played by the social media entity in creating and benefiting from viral violent content nor does it address anything new or significant regarding the exemption of such entities. What these intended to do to prevent OGBV has only turned into a cat-and-mouse game, thus not really addressing the widespread powers of social media entities. Here, courts, especially at the high court level, play a significant role in addressing the overall harm and collective solutions required to prevent OGBV.

It is high time that the regulatory approach to social media platforms in India address the harm caused by the logic of the attention economy underpinning the operation of these platforms, which makes its algorithms prioritize virality and sensationalism. The press note released by the Ministry of Electronics and Information Technology (MeitY) rightly pointed out the issue of virality. Unfortunately, it did not translate into any concrete amendment to the IT Rules, 2021, other than requiring a quick turnaround for user complaints. As noted earlier, the harm from OGBV is often exacerbated by the techno-design choices of platforms that actively promote such harmful content to profit from users’ attention. Hence,
as IT for Change recommended in a recent research report, “Regulatory oversight over moderation practices of platforms must not be limited only to decisions to takedown or reinstate content, but must also extend to design choices and algorithmic processes of amplification of content.” In other words, social media platforms should be held responsible to ensure that the operation of their algorithms does not cause harm or violate the rights of their users. More than controlling what their users post, upload, or share, these platforms are better equipped to cause their organizing, curating, and recommending functions to not facilitate, amplify, and exacerbate harmful content.

The proposed Digital India Act is expected to change the safe harbor protection regime as the MeitY is considering extending such protection to all types of internet intermediaries. In fact, the amendments to the Intermediary Rules under the IT Act were an early signal of the government’s intention to impose stringent due diligence requirements on intermediaries, such as social media platforms. While the dumb conduit metaphor underlying the safe harbor regime no longer accurately applies to the form and function of many intermediaries today, concerns have been raised that the absence of liability protection for intermediaries can jeopardize the free speech rights of users as intermediaries engage in overzealous censorship to escape liability.

Through our study, we were encouraged by the courts’ acknowledgment of holding intermediaries liable. We hope that this will result in steps towards reducing violence and enable better access to justice for survivors.

3.5 Finding 5: Courtrooms continue to be sexist and patriarchal spaces for survivors of OGBV cases, thereby perpetuating common judicial stereotypes and impacting access to justice

Dignity is a key attribute for the framework of understanding rights affected in cases of OGBV. The Cambridge Dictionary defines dignity as, “The importance and value that a person has, that makes other people respect them or makes them respect themselves.” The value being referred to here is intrinsic to a person on account of being a human being and is captured in various human rights frameworks, including the fundamental rights guaranteed by the Indian Constitution. The nine-judge bench of the Supreme Court in Puttaswamy, noted, “Dignity is the core which unites the fundamental rights because the fundamental rights seek to achieve for each individual the dignity of existence [...] Privacy ensures the fulfillment of dignity and is a core value which the protection of life and liberty is intended to achieve.” Given that these rights are enshrined under Article 21 of the Constitution, they extend to non-citizens too.

However, dignity has not always been accorded in the same way to marginalized groups. Marginalization and its impact can vary based on geographic location, social context, and
background. In the larger history of liberal societies, dignity has also focused on gender and been
only accorded to those whom the patriarchy deems important. Syliva Walby defined patriarchy as, “A
system of social structures, and practices in which men dominate, oppress and exploit women.” Any
perceived transgressions to these social structures open women up to harassment, ridicule, abuse,
assault, or even death, in extreme situations. These gender roles and expectations intersect with
other forms of marginalization along the lines of gender identity, caste, class, race, religion, sexuality,
disability etc. When a person lies at these intersections, they face the possibility of increased
vulnerability.

Sexism can be usually defined based on two components: “Hostility towards women and endorsement
of traditional gender roles.” Courtrooms also replicate these structures, especially in gendered
offenses. In her book, Pratiksha Baxi noted, “The rape trial does not merely reflect patriarchal norms,
but it also imparts a ‘specific disqualification of women and women’s sexuality.’” The evidence from
our research points towards not just hostile or casual instances of sexism but also benevolent sexism,
which emphasizes men’s role as protectors of women. While it is the judiciary’s role to protect the
rights of all people, it often gets rooted in existing notions of gender and is interpreted as the
protection of patriarchal qualities, such as ‘honor’ and ‘modesty’, in cases of OGBV.

The Indian criminal justice system is based on colonial legislations that are still applicable with limited
amendments, like the IPC, with amendments on sexual offenses in 2013, or the IEA, with some
additions on electronic evidence. As a result, the Indian legal system comes with Victorian biases.
This introduces a dual discrimination in the way women are treated in cases of sexual assault in India:
first, by drawing on ‘imperial patriarchies’, and second, by deeming a native woman’s testimony non-
credible. So much so that the ‘immoral character’ of women was once hard-coded into the now-
deleted Section 155(4) of the IEA, which stated, “when a man is prosecuted for rape or an attempt to
ravish, it may be shown that the prosecutrix was of generally immoral character”. This was used as a
means of discrediting a woman’s testimony. While this provision was repealed in 2002, the use of a
woman’s sexual history to question the integrity of her evidence continues to be a factor in cases of
sexual offenses, whether offline or online. The rape law in India specifically suffers from severe
stereotyping and patriarchal markers of typifying the ‘ideal victim’ (or victims whom courts will believe)
and requirements of “sterling testimony”. These have also led to the perpetuation of rape
myths, which are “prejudicial, stereotyped, or false beliefs about rape, rape victims, and rapists”.
Some common rape myths identified by Jennifer Temkin have been listed below.

1. Rape by a stranger is more traumatic than rape by an acquaintance.
2. Genuine rape victims/survivors report the incident to authorities without delay.
3. Victims/survivors of rape are visibly emotional when recounting their experience.
4. Women frequently make false allegations of rape.

5. Women always physically resist rape, which leads to injuries to their bodies and genitals.

During the course of this study, a key observation was that sexist stereotypes continue to prevail, both among judges and the lawyers arguing before them. This aligns with previous studies that have established the patently hostile spaces courtrooms can be for women in cases of sexual violence. The language of court orders is an important facet to understand innate judicial biases. Written orders and judgments of courts hold them accountable, especially since they are capable of scrutiny through further court processes, like reviews, appeals, or public critique. In this context, the content of these orders, including the direct decision and reasoning, becomes significant. Changes to sexist judicial language to enable a more gender-just space have also been requested by stalwarts of the feminist movement in India, like Indira Jaising in her open letter to the Chief Justice of India.

This is not to say that the judiciary is oblivious to the issue of sexism towards survivors of gender-based offenses. In March 2021, the Supreme Court in the Aparna Bhat ruling, set down guidelines to ensure that bail conditions imposed by courts do not include a compromise between the accused and the victim/survivor. Additionally, the Supreme Court asked all courts to be sensitive towards victims/survivors in cases of gender-based violence to avoid traumatization of the victim/survivor during the proceedings or the arguments. The court went on to state that in cases of sexual violence, women also get blamed for the attack, especially given the prevalence of myths and stereotypes. The court verdict stated:

“Judges can play a significant role in ridding the justice system of harmful stereotypes. They have an important responsibility to base their decisions on law and facts in evidence, and not engage in gender stereotyping. This requires judges to identify gender stereotyping, and identify how the application, enforcement or perpetuation of these stereotypes discriminates against women or denies them equal access to justice.”

This is a welcome decision from the highest court of the country and needs to be incorporated by the judiciary in letter and spirit. Additionally, in August 2023, the Supreme Court released a ‘Handbook on Combating Gender Stereotypes’ to prevent them from being perpetuated. Its efficacy remains to be seen, but it is a step in the right direction.

In this section, we have taken examples of cases where the court passed favorable orders to protect rights of women in cases of online violence but retained certain stereotypical and gendered social considerations to arrive at such decisions. These cases are a few examples from our study which reflect what earlier studies have proven, that court decisions can be sites of upholding sexist notions.
3.5.1 Putting women on a pedestal: *The Present Petition v. Unknown*²⁵⁸

**Facts of the case:** The case was an anticipatory bail application filed by the petitioner on being implicated in a complaint under Section 354D and 509 of the IPC read with Section 4 of the Tamil Nadu Prohibition of Harassment of Women Act, 1998. The petitioner was charged on account of harassing several women on social media platforms, like Facebook and Twitter/X, through “scandalous and derogatory” posts and tweets. As such, the court also noted that in such a case, the court’s role is to arrive at a prima facie determination of whether the petitioner committed these offenses.

**Decision of the court:** The court declined the request for anticipatory bail in view of the derogatory comments made by the petitioner against the respondent–complainant. The court went on to note that anticipatory bail may impact fair and effective investigation, and so due caution was to be taken before granting the same.

**Critical analysis of the decision:** This was a case of anticipatory bail and, as the court noted, it would have been enough to show a prima facie possibility of the offense being committed by the petitioner. However, the court’s decision went beyond this. As Section 509 was applied in the complaint, the notion of modesty of women was introduced in the decision. The decision offered a strange amalgamation of two perspectives. It delved into the question of individual privacy in relation to the online space but also focused on how modesty of women is impacted because of harassing posts. In that regard, it is useful to extract the portions from the ruling to understand the emphasis on a woman’s modesty and the need to protect the same.

> “Even a bare reading of the said posts leaves a sour taste in the mouth of this Court, as those statements are overly derogatory in nature and it demeans, the modesty and chastity of the women folk […] It has been oft said that the essence of a woman’s modesty is her sex. The culpable intention of the petitioner is the crux of the matter and the reaction of the general public in this regard is very relevant and so also that of the woman against whom such scandalous posts are made. Modesty is an attribute associated with female human beings and it is a virtue which attaches to a female owing to her sex.”

This discourse on the modesty of a woman is extraneous to the decision in an anticipatory bail plea and takes an antiquated view of the rights of the woman in question. While a strict approach to bail pleas may be needed in cases of OGBV, it must arise from a rationale rooted in rights like privacy or the ability to participate online rather than the modesty of a woman.
3.5.2 Good decision, bad terminology: Guruvinder Singh v. State of Uttar Pradesh

**Facts of the case:** The bail applicant in this case was accused of taking ‘obscene’ photos and videos of the victim/survivor, in addition to committing sexual assault. The bail applicant also used the photos and videos to continue sexually assaulting the victim/survivor. The applicant’s bail plea rested on the fact that it was not rape and that the victim/survivor had, in fact, been in a consensual relationship with him and provided several witnesses to the effect. It was also stated that the bail applicant had shared explicit photographs with the victim’s/survivor’s mother and sister.

**Decision of the court:** The court rejected the bail application. It focused on two important aspects, which are also key to this study, the dignity and privacy of individuals. The ruling also noted that the court must act as parens patriae to protect the fundamental rights of people against illegal use of sexually explicit images and videos.

**Critical analysis of the decision:** It is significant to note that even in an order for bail, the high court judge is able to focus on the question of dignity and privacy of the victim/survivor who was being targeted through sexually explicit images and videos. It goes to show that such rights-based considerations can be made in cases of bail, which are often meant to be cut and dry. It is also significant that the court understood that gendered dynamics affect women more, as is evident in the ruling, which noted, “In most of the cases, like the present one, the women are the victims.” However, it is also important to note that the verdict still uses language around, “outrag[ing] the modesty of the woman”—concepts that have been critiqued in this study.

3.5.3 Emphasis on tradition, not rights: Robin Sharma v. State of Punjab

**Facts of the case:** This case included anticipatory bail applications filed by persons against whom FIRs had been filed under Sections 354D, 503, 509, 384, and 511 of the IPC along with Sections 66D, 67, and 67A of the IT Act. In one of the complaints, it was alleged that the second accused had used communication platforms, like WhatsApp, to send the complainant, “objectionable, vulgar messages, forged, fabricated morphed photographs” and to make unwanted voice or video calls. In another FIR, complaints were made against both the first and second accused on grounds of “creating fake IDs of complainant on Facebook, Snapchat and Instagram” as well as posting objectionable photographs and defamatory content with the intent of coercing the complainant to enter into physical relations with the second accused.

**Decision of the court:** The bail petitioners chose to withdraw their petitions so the case was to be closed. However, the court chose to incorporate certain observations in its order, which included instruction to the police to take prompt action in cognizable cases and not cause unnecessary delay, which would enable the court to exercise its jurisdiction.
Critical analysis of the decision: Once again, the court is not remiss in recognizing the systemic and systematized violence faced by women. The court went beyond the ask in the anticipatory bail ruling to insist on the importance of the investigating authority, i.e., the police. The court also recognized that privacy of individuals is paramount. Even as it did so, one of the threads on which the court rested its progressive and sensitive notes about investigation, was based on our “ancient civilisation and culture”. Arguably, these are not rooted in laws and rights, but a social and cultural understanding of gender and discriminatory practices. The court noted:

“In this land of ancient civilization and rich culture governed by fundamental principle that no society can prosper without respect for women expressed by [the] Sanskrit shloka [sic] ‘Yatra naryastu pujyante ramante tatra Devata’ women are now victims of heinous crimes and subjected to domestic violence, cruelty/maltreatment and sexual harassment and due to these evils, need effective protection of law administered by all agencies of State with an iron hand.”

Such reliance on sociocultural or religious practices or beliefs often harms such judgments, especially where rights of victims/survivors are implicated.

3.5.4 Expectations from “prudent women”: Mohammad Nasar v. State of Andhra Pradesh

Facts of the case: The bail applicant sought anticipatory bail, as the complaints against him were in the nature of posting illegal photos of the complainant on social media and continuing to do so after being released on bail the first time.

Decision of the court: The court rejected the bail application, especially because it was a recurring offense.

Critical analysis of the decision: The decision of the court to rely on the repeated nature of the offense was useful. However, the court noted with regard to the uploaded photographs that, “No prudent woman would post her nude photographs in social media.” While seemingly innocuous, this statement relies on a stereotypical trope to derive the direction in which the court should move regarding the case. Additionally, it creates an expectation of what a ‘prudent woman’ does, which means anything outside of such expectation may not receive similar treatment in courts.

The key outcome of this section is that courtrooms continue to perpetuate the same, decades-old gendered myths and stereotypes, although they have been perpetrated alongside an astute recognition of the dynamics of OGBV. Regardless, these myths exacerbate the challenges of the online space, like quick dissemination of non-consensual intimate images or the availability of personal information of potential victims/survivors.

The inability of a courtroom to be sensitive as well as fair and feminist in its outlook is a major obstacle towards achieving effective access to justice for women. Even in cases where courts have been
cognizant of the impact of gendered offenses, like the ones discussed in this section, it is imperative that verdicts remain rooted in rights-based principles and do not take on stereotypical and paternalistic tones.

The way forward must involve training judges and lawyers early on to identify these myths and stereotypes to prevent them from being repeated and perpetuated—this is also a recommendation from the Supreme Court in the Aparna Bhat verdict. Judicial training curriculum must not shy away from adopting a fair, just, and equitable framework for the rights—embedded in constitutional principles of equality, right to life with privacy and dignity, and freedom of thought and expression—of women and people from marginalized genders.

It is imperative for such trainings to happen at all levels of the judiciary, including the Supreme Court, given certain decisions that have reflected anti-rights-based perspectives even from the highest court (as in the case that defined a “sterling witness” or what the modesty of a woman entails). It is important for judges to be cognizant of their unconscious biases and their impact on the important work of providing justice.

### 3.6 Finding 6: Courts fail to recognize power differentials among perpetrators and survivors in OGBV cases

The digital sphere, which is a breeding ground for patriarchy, reinforces power structures typically seen in real life. The ubiquitous online world has resulted in newer opportunities for perpetrators to attack women using technology, leading to increased risk for women on the internet,\(^{262}\) as can be seen from the cases in this study. Forms of sexual violence and harassment stem from socially constructed beliefs and attitudes about gender and sexuality, which fulfill perpetrators’ desires for power and control.

The Supreme Court, in the Aparna Bhat verdict noted that the “causes and factors of violence against women include entrenched unequal power equations between men and women that foster violence and its acceptability, aggravated by cultural and social norms, economic dependence, poverty, etc.” The systemic gender gap along with years of patriarchal and social forces allow some individuals to exercise power over others, thereby exerting control over even the simplest of relationships in society, including those in educational institutions, families, and romantic relationships.
In Figure 2, based on relationships between the accused and the victims/survivors from our sample cases, we have categorized the reasons for the perpetuation of violence, how it is perpetrated, and the kind of relationships in which power is misused.

The most common theme emerging from all the cases we reviewed was the misuse of the fiduciary relationship by an older man against a younger person, in some cases minors and mostly women. Fiduciary relationships are “relationships based on trust” or ones where confidence is reposed by one person on another, which leads to a “transaction in which there is a conflict of interest”. The law determines the existence of a fiduciary relationship by making it the duty on the person in whom such confidence is reposed, as seen in laws like POCSO. These duty holders include family members, teachers, superiors, or colleagues at work and people in positions of power, like police officers. For instance, in the case of State v. Pankaj, the accused was the elder brother-in-law of the victim/survivor. In the case of Susil Kumar Mohanty v. The Victim, there was an age difference of 15
years between the accused and victim/survivor. In other cases,\textsuperscript{268} minor girls between the ages of 13 to 16 were the victims/survivors.

In most cases, we found that there was a direct misuse of these positions of power resulting in violations or lack of free consent. In \textit{Amit Raosao Patil v. State of Maharashtra}, the Bombay High Court\textsuperscript{269} observed that when consent is induced from a person due to the nature of a fiduciary relationship, it will not be treated as free consent on the victim's/survivor's part.

The lack of autonomy for women and girls in our rigid patriarchal societies makes it difficult for them to stand up for themselves and stop the abuse coming from people in such positions.

Some of the common relationships with power dynamics that we identified through our sample cases have been listed below and discussed in the following sections.

1. **Familial relationships:** Relationships within families or related by marriage, blood, or adoption

2. **Intimate relationships:** Relationships between partners, including unmarried couples, couples who have decided to marry, etc.

3. **Workplace relationships:** Relationships between people in workplaces, including colleagues, or seniors/juniors

4. **Teachers or instructors and their students:** Relationships between teachers and their often-minor students

### 3.6.1 Familial relationships

Even modern gender-structured family systems unjustly distribute burdens and benefits based on gender roles.\textsuperscript{270} The proximity of committing an offense also increases inside family systems where older men take advantage of their position of power to threaten and intimidate younger members, usually women, to carry out acts that they would not otherwise do.\textsuperscript{271} Some instances from our sample set of cases where there was an abuse of power within families have been listed below.

1. In \textit{State v. Pankaj}, the accused stalked and threatened his wife's minor sister (the victim/survivor) to engage in sexual relations with him. The accused threatened the victim/survivor under the pretext of sharing non-consensual intimate photos and videos of her, which then led to rape.

2. In \textit{Vikash Rajak v. The State of Madhya Pradesh},\textsuperscript{272} the accused, a relative of the victim/survivor, made a fake Facebook ID and circulated the profile to defame her.
3. In *Mool Chand v. Nathu Lal*, the victim/survivor alleged that her cousin’s husband (the accused) took blank cheques from her, regarding an LIC claim, set up dishonor of cheque cases against her, and used them to sexually assault and rape her. He also threatened to release intimate photos of her on the internet if she told anyone.

These examples reveal the carefully constructed situations that are developed against the backdrop of shame within the family and society. The powerplay in these cases directly links back to the positions of power held by perpetrators (who are generally men, based on the findings of this study). The perpetrators used the threat of posting intimate photos of the victims/survivors on the internet to shame women or with the intent to defame them, knowing this would embarrass or humiliate their families in a patriarchal society. Consequently, the women felt coerced into silence to avoid such ignominy.

Further, age differences between the family members create a power imbalance in relationships, particularly in patriarchal societies where age and seniority demand higher levels of respect in society. Many women enter into a relationship with the mindset that people senior to them in age or rank should always be treated with deference or respect. They are also made to believe that failing to show family members in positions of power the prescribed form of respectful etiquette or not carrying out their reasonable requests may be regarded as reprehensible and punishable. This means that in any form of familial relationship where one person is relatively older than the other, the younger member often feels traditionally bound by honor to obey and submit to the authority of the older person. Thus, it is unsurprising that all the accused in the cases mentioned earlier were men who targeted younger women and girls within their families.

3.6.2 Intimate relationships

A study by the European Institute for Gender Equality (EIGE) discusses how gender-based violence, including intimate partner violence, affects women disproportionately, as it is a manifestation of the power imbalance between women and men. Even today, globally, women form the overwhelming majority of the victims/survivors of intimate partner violence. Partner violence against women is more prevalent in patriarchal societies and is a result of unequal power relations that emphasize gender roles, including the dominance of men over women.

Our sample set included cases where partners issued threats, made false promises, and used intimidation through different modes of technology, to coerce their partners to do something or committed direct acts of violence against the victims/survivors. Some examples of cases from our sample set where the accused used technology to inflict violence and assert control over women have been listed below.
1. In *Mrs. Rehana Begum v. The Inspector of Police*, the accused and victim/survivor met via a matrimonial website. The accused sent abusive messages and threatened to upload obscene images of the victim/survivor online. The court granted the accused bail with the stipulation that he should refrain from contacting the victim/survivor.  

2. In *Smt. Ranjana Chaudhari v. State of U.P. & Another*, the accused was married but promised to marry the victim/survivor once she turned 18. Once she found out about his marriage, she refused to marry him. In response, the accused threatened to upload an intimate video of the victim/survivor.

3. In *Pachipala Prabhakara Rao v. State of Andhra Pradesh*, the accused told the victim/survivor, who was his colleague, that he loved her and wanted to marry her while hiding that he was married. They engaged in sexual intercourse after he promised to marry her, and later, he got access to her intimate photographs. Once the victim/survivor got to know about the marital status of the accused, she wanted to complain to her higher-ups at work. In response, the accused shared her intimate images on WhatsApp groups with their superiors to shame her. He also used a caste slur while sharing the images.

4. *Ms. X v. State & Ors.* was a case related to the removal of web pages with sexual content featuring the victim/survivor. The accused and the victim/survivor met in school and became close friends. The accused was possessive of her, did not let her talk to others, and often snatched her phone to check her messages. She alleged that the accused started emotionally blackmailing her and compelled her to send her intimate photographs to him. He threatened that if she did not do as he asked, he would commit suicide. She succumbed to these tactics and sent him her intimate pictures. She stated that her relationship with the accused was very abusive, and, therefore, she ended her relationship with him. The accused, then, threatened her and followed her to the place of her higher studies.

5. In *Mohammad Nasar v. The State of Andhra Pradesh*, the accused took nude images of the victim/survivor during their intimate relationship and posted them on social media. When the victim/survivor filed a case, the accused threatened to release more pictures once he was released on bail. He later uploaded additional images of her on a fake social media profile.

As examined through multiple studies, victimization in intimate relationships is more common among women with lesser power in their relationships. Furthermore, devices, applications, social media, and internet platforms are used as tools of oppression by intimate partners to cause harm. Threats and intimidation using technology to assert control over partners are prevalent in cases of intimate partner violence. Even if the victims/survivors increase their privacy settings or block such
perpetrators, the degree of personal information shared through intimate relationships is higher than interactions with strangers, which makes it more difficult to mitigate the potential harms.289

### 3.6.3 Workplace relationships

Sexual harassment at the workplace is a form of violence where the perpetrator, who may hold any position at the same workplace as the victim/survivor, is emboldened to exert power and harass the victim/survivor.290 Quid pro quo sexual harassment works on the premise of exerting power for a beneficial exchange or to prevent harm at the workplace, thereby creating hostile workplaces for victims/survivors.291 We came across one such case in our sample set.

1. In *State v. Ajay*, the accused, who works with her, drugged and sexually assaulted the victim/survivor. A week later, the accused informed the victim/survivor that he had made an intimate video of her, which he would post online or kill her if she complained.292

2. In *Pachipala Prabhakara Rao v. State of Andhra Pradesh*, as discussed in the previous section, the accused told the victim/survivor, who was his colleague, that he loved her and wanted to marry her while hiding that he was married. Once the victim/survivor got to know about the marital status of the accused, she wanted to complain to her higher-ups at work. In response, the accused shared her intimate images on WhatsApp groups with their superiors to shame her.293

Harassment by a person in a position of power can have significantly harmful consequences for victims/survivors, as opposed to being harassed by someone without power.294 For instance, in *Crime No. 1021/2015 Of v. By Adv. Sri. Sasthamangalam*,295 two doctors filmed babies being delivered in their place of work and distributed these videos on social media, WhatsApp, and other visual channels. The accused—a gynecologist and an anesthesiologist—held a fiduciary position but were granted bail in the case.

Abuse of power to control and sustain power inequalities has been a concern in many workplaces over the years.296 In 1992, Bhanwari Devi, a Dalit woman who was a social worker with the Rural Development Program of the Government of Rajasthan, was gang raped for doing her job. This case highlighted the extent of sexual harassment incidents in India's workplaces. It struck a chord with the nation and revealed the hazards faced by women in the workplace. A writ petition, popularly known as the *Vishaka* case, was taken up in the Supreme Court.297 This case led to the introduction of guidelines for sexual harassment at workplace. This was the foundation for The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013. This law took account of the practical issues arising out of vertical (with managers and superiors) and horizontal (between colleagues) power dynamics at the workplace. In *Apparel Export Promotion Council v. A.K. Chopra*,298 the Supreme Court
upheld the dismissal of a superior officer of the Delhi-based Apparel Export Promotion Council for sexual harassment. The court expanded the definition of sexual harassment to state that “physical contact is not always essential for an act amounting to workplace sexual harassment”. This verdict plays a significant role till date, as sexual harassment can now happen in the online public sphere and can include any ‘unwelcome’ act that does not necessarily involve physical contact.

Workplaces where men hold positions of power and misuse them against women lead to unsafe and hostile work environments. Further, research shows how the intersection of gender and power in the workplace results in women being targets of harassment, particularly when they step out of perceived gender norms, such as by moving into positions of authority and/or historically male occupations. This has a trickle-down effect on the entire work culture, as can be seen from multiple cases in India—including Tarun Jit Tejpal v. The State Of Goa and Mobashar Jawed Akbar v. Priya Ramani—as well as public narrations of hostile work cultures outside India, like Susan Fowler’s experience at Uber.

3.6.4 Teachers or instructors and their often-minor students

At its heart, education is a space historically rooted in systems of power. The role of a teacher or instructor in Indian culture comes from a form of authoritarianism where the student is assigned an inferior status to ensure that they receive a good education. Students are taught to hold teachers in high regard and treat them with utmost respect regardless of their competence or behavior. Our case study included instances where teachers, be it in schools or private tuitions, misused their position of power to inflict harm on their students, who were often minors. Two such examples have been listed below.

1. In Sharat Babu Digumarti v. Govt of NCT of Delhi, the accused took photographs of the prosecutrix, a 16-year-old girl the accused was supposed to be tutoring, holding a beer. He then threatened to release that photograph on the internet if she did not meet him. When she met the accused, he sexually assaulted her.

2. In State v. Lalit Kumar, the accused, a tuition teacher, sexually harassed the victim/survivor, a minor student, and sent her messages via phone and on Facebook. The accused also threatened a witness with dire consequences for backing the victim/survivor.

In these cases, it is evident that apart from misusing their fiduciary position, the accused threatened and intimidated their students to solicit a coerced response from them. In 2016, a study by the Women and Equalities Committee of the UK Parliament reported that, “29% of 16–18-year-old girls had experienced unwanted sexual touching at school”. An analysis of India’s National Family Health Survey found that over 10 million women in India had been sexually abused by a teacher when they were in
Those in positions of authority, trust, and power over students routinely sexually harass students in India. Furthermore, public discussions of sexual matters, especially relating to children, is largely taboo. Such violence often becomes a barrier to increasing girls’ educational participation in India. Despite the child sexual abuse law in India addressing teachers, in particular, to address the coercive power they have over minor students, there is very little protection for students against abuses of power in places, like tuition centers, with minimal supervision and one-on-one student–teacher interactions. Teachers and instructors have significant power over students. A common trend in our sample set of cases was that of tuition teachers using technology—threatening to sharing intimate images on the internet—to shame adolescent girls into sexual activities.

Our case study exposes situations where persons abuse their authority, particularly with minors, emphasizing the urgent need for comprehensive educational safeguards. Despite existing laws addressing teacher-student dynamics, students' vulnerability in minimally supervised settings remains a pressing issue. These cases underscore the disturbing trend of exploiting and coercing students through technology, necessitating comprehensive solutions for student safety and well-being.
Chapter IV: Conclusion and Recommendations

This empirical investigation has attempted to understand judicial responses to cases of OGBV in India. While going through the cases, we realized the need to engage with regressive social norms that still persist in judicial systems. Judicial stereotyping has played a significant role in the outcome for cases. While unravelling the complexities of accessing justice, we came across the significant issues of the non-recognition of the online continuum in courtrooms and the judicial attitudes towards online crimes. Legal institutional challenges need to be all encompassing and recognize the additional concerns presented by the online public sphere when addressing the multiple barriers for women accessing justice—including sexist courtrooms, multilayered power differentials, and the non-recognition of possible and emerging gendered hate speech offenses. Despite the rights of privacy and dignity being recognized through landmark cases, like *Puttaswamy*, our legal institutions are failing women. A combination of factors from the outdated texts of the laws to the social mores that pervade courtrooms is causing these seemingly improved circumstances for women to take a backseat in cases of OGBV. The conversation around these issues has also been framed in the gender binary because our laws fail to recognize the additional layers of discrimination transgender and other gender identities face.

The massive issue of the normalization of online violence—including lack of effective redressal mechanisms, low enforcement by the government, and options afforded by the anonymized internet—has incentivized a multiplicity of violent online behaviors. The challenges presented by the hegemonic cultures of misogyny in the online public sphere require appropriate legislation as well as institutional changes.

In order to keenly understand the concerns of adjudicating OGBV, it is imperative to realize the social structures at play in these behaviors. In essence, women’s right to participate in the online public sphere is constantly at odds with society’s need to control them. Finding a safe space and a voice online is often risky for women, especially those who are multiply marginalized, at the intersections of caste, religion, race, gender identity, sexual orientation, and disability. In the absence of a safe space, survivors of online violence are unable to access the justice system effectively to address their concerns. This is despite the fact that the judiciary has often laid out the rights afforded to all people by our constitutional regime.

As such, the sum and substance of the rights of individuals, especially women, non-binary people, and other marginalized groups, has already been captured in the Indian Constitution. Articles 14 and 21 elucidate the rights to equality and equal treatment before the law and the rights to life and personal liberty, respectively. These rights have been given their contours and nuances through several landmark cases, including the *NALSA decision* (on rights of transgender people), the *Puttaswamy*
verdict\textsuperscript{315} (on the right to privacy), the \textit{Vishaka} judgment\textsuperscript{316} (on the protection of women against sexual harassment at workplace), the \textit{Suresh Koushal} verdict\textsuperscript{317} (reading down Section 377 of the IPC to prevent the harassment of LGBTQIA+ individuals).

What we witness, then, as a failure and an impediment to justice, is a misrecognition\textsuperscript{318} of pre-recognized rights. Courts, as institutions of justice, should not obfuscate a violation of privacy by qualifying it through patriarchal provisions of modesty or by making an overreaching sexist interpretation of the modesty of a woman. This unsettles and destabilizes existing rights, defeating the discourse of a rights-based approach to gender-based violence. This study offers proof that when courts move to understand the societal harm perpetrated through OGBV on the foundation of established rights, rather than on social, moral, and patriarchal norms, a glimmer of justice that may be visible to the victims/survivors of such harm.

While rethinking legal-institutional responses to effectively address systemic violence online, some core concepts of the law that regulate issues of OGBV need to be questioned. The legal system, including the judiciary and the legislature, needs to take responsibility for addressing the challenges highlighted in this study. Policy changes should focus on justice and inclusivity in the digital age, capitalizing on the current consensus for effective reforms.

Global debates increasingly point to the need for platform accountability mechanisms. Liability and due diligence frameworks for business and human rights violations, including amplification of content on platforms and impacts on users, are emerging as key concerns.

While Indian courts have appointed experts to address content takedown issues in certain cases, more needs to be done to holistically tackle the larger platform ecosystem. The move to address platform regulation through the introduction of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as well as the proposed Digital India Act, which intends to replace the 23-year-old parent legislation - the Information Technology Act, 2000 - is a vital step. However, the regulatory framework requires extensive and ongoing public debate, inter alia, to also ensure that platform intermediaries with disproportionate market power can be held accountable for their duty of care towards users.

The following sections discuss some overarching areas where we need to rethink our approach based on this study.

\textbf{4.1 Courts must recognize the importance of the online public sphere and give equal importance to online gendered offenses}

1. The study has shown that, in many cases of mixed online and offline offenses, the focus of the case shifted to the offline offense. This traditional understanding of the harm that is focused
only on visible injury cannot be the driving force in judicial decisions anymore. There is an urgent need to address the online–offline continuum in the courts and give equal importance to hybrid offenses while adjudicating a case.

2. There is an urgency to stop the trivialization of OGBV. Courts need to recognize the import of online offenses, treating them as implicating the body and personhood of the victim/survivor. This includes understanding the online-offline continuum and addressing hybrid offenses appropriately.

4.2 NCIID requires specific and dedicated steps for redressal, including from courts as well as the legislative process

1. Courts must establish robust procedures for effectively addressing the online circulation of non-consensual intimate content. Courts should set down guidelines and rely on appropriate legal precedents to handle NCIID, involving privacy rights protection and recognizing emerging digital crimes. This can follow the judicial practice of recognizing systemic harms and rights of victims/survivors as seen in many pathbreaking decisions like the Vishaka ruling or the NALSA verdict. While courts have appointed experts to tackle content takedown issues, stalling the proliferation of NCIID material is an uphill task.

2. Superior courts are slowly recognizing the need to pass effective orders to minimize online recirculation of non-consensual, sexually-explicit videos and images. A handful of orders in our sample cases noted the challenges to swiftly pulling down such content, especially given the coordination required between state agencies and online intermediaries. It may be time to assess if processes to take down NCIID material can be as prompt as often seen in copyright takedowns in India.

3. The applicability of Article 21 against non-state actors has been recognized in the Kaushal Kishor case. This creates scope for the right to privacy, including the right to be forgotten, to be protected and upheld in cases of NCIID. A few courts have been cognizant of this and have, in fact, asked for these rights to be pursued by the victims/survivors/prosecutrices in the cases.

4. Courts should recognize emerging forms of crimes like NCIID as distinct concepts and handle them appropriately by leveraging existing legal provisions. This recognition is essential for understanding the complex online-offline nature of these crimes. While having dedicated legislation, such as the New South Wales law, would be ideal, introducing additional criminal law provisions in the Indian legal system could potentially complicate matters further. Instead, a more holistic approach should be adopted by the courts to address NCIID as a societal issue. This approach should include explicit references to NCIID and its unique challenges, thereby
creating legal precedents and guidelines for handling such cases effectively. The *Vishaka* judgment serves as a notable example of how the courts can play a pivotal role in recognizing and addressing emerging and urgent issues, eventually leading to the formulation of dedicated laws. While the proposed Digital India Act may offer civil remedies, there is a pressing need to define online harms comprehensively. This involves determining the specific types of online harms associated with NCIID cases to ensure that the legal framework is well-equipped to tackle these evolving digital crimes.

### 4.3 Courts must move beyond misplaced notions in OGBV cases and deliberate on reforming institutional processes and procedures

1. Courts should uphold victims'/survivors' right to privacy in OGBV cases, even where provisions on 'outraging the modesty of a woman' have been used. Such provisions also need revision and require consultations with women's rights groups and civil society working towards gender justice.

2. Courts should uphold the right to privacy of a victim/survivor in cases of OGBV and take a more holistic understanding of privacy – as comprising informational, physical, and decisional agency.

### 4.4 Courts must not let procedural hurdles, including digital evidence certification, impede proper justice delivery and must contextualize bail orders for the online space

1. Courts must use their power under the CrPC to direct parties to produce the Section 65B certificate supporting secondary electronic evidence, if the same is missing. Evidence should not be dismissed merely because this certificate has not been produced. Such safeguards will ensure access to justice for victims/survivors is not barred because of procedural lapses. Even if the new evidence bill comes into force, there is a requirement for a certificate to authenticate electronic evidence. This recommendation would apply in such a case.

2. Courts should incorporate contextual considerations related to the internet, social media platforms, or technology/communication devices when issuing bail orders. Presently, bail conditions do not address the distinct needs to address the distinct needs of cases involving OGBV, where perpetrators utilize online communication methods to target victims/survivors. These conditions, which may include restrictions on contact between involved parties, must preserve the fundamental right to freedom of speech for the accused while also effectively preventing online revictimization.
4.5 Courts must identify challenges in holding digital platforms accountable for profitable viral content

1. Courts should hold online platforms accountable for harmful content. Intermediaries play a major role in spreading online violence. Given their engagement-based business model, they are not dumb conduits for transmitting information, and the courts have started recognizing this. Consequently, the extent of responsibilities to be imposed on intermediaries need to be examined. The IT Rules, 2021, have done this to an extent, but regulation needs to be more holistic while also holding sufficient public engagement.

2. Courts should recognize the role of social media companies in profiteering out of the viral circulation of content, and address algorithmic amplification of content that undercuts dignity and rights of users. By acknowledging the algorithmic processes of curation, recommendation, and hiding of content, courts can highlight the many ways in which platforms regulate content, in pursuit of their specific (profit-oriented) goals. Step change is possible only with comprehensive changes to the policy and legal regime targeting large digital corporations, including for algorithmic accountability. This is critical to move away from penalizing individual offenders and bring about systemic change for women's equal participation in the online public sphere.

4.6 The criminal justice system must undertake ecosystem-level changes in sensitization and inclusive policies

1. Courts must be inclusive spaces for marginalized groups. Courts must ensure that they become safe spaces for women, non-binary people, and other marginalized groups, including those persecuted for their caste, to seek justice.

2. Courts must recognize power imbalances due to social and cultural factors during adjudication.

At this moment in India’s digital history, there seems to be some emerging consensus to address problems of the technological world. It is imperative for the policy ecosystem to capitalize on this moment and create space for effective change focused on justice. The legal system—both the judiciary and the legislature—must take the responsibility to address the concerns highlighted in this study.
Endnotes


3 When violence is carried out using technology and communication equipment, including hardware and software, such as smartphones, cameras, and other recording equipment, GPS (global positioning system), or satellite navigators, etc., it is commonly referred to as TFGBV. This is a broader term used internationally. However, for the purposes of this study, we are referring to more cases of OGBV, as the violence in these cases has been perpetrated via the internet and online networks.


12 Research conducted by the International Center for Research on Women (ICRW) and Quilt.AI in 2020 on online violence in India showed that online violence on Twitter/X tripled during the pandemic from 26% to 74%. More importantly, the study found that even when people look for help, they have access to limited local resources. Instead, they are redirected to foreign websites or taken to local services like law firms and the Indian government cybercrime websites. See, International Centre for Research on Women, & Quilt.AI. (2021). COVID-19 and online violence in India: Digital intelligence report. https://www.icrw.org/wp-content/uploads/2021/10/Online-Violence_Full-Report-Quilt.AI-and-ICRW.pdf


14 In this study, we’ve retained the use of victim/survivor because while the word ‘victim’ is often used in legal and therapeutic contexts, especially for someone who has initially suffered harm, the term ‘survivor’ denotes agency and existence beyond the traumatic experience. In certain instances, only ‘victim’ has been used when it has been referred to by case/order. See, Victim or Survivor: Terminology from Investigation Through Prosecution. (n.d.). Sexual Assault Kit Initiative. https://sakitta.org/toolkit/docs/Victim-or-Survivor-Terminology-from-Investigation-Through-Prosecution.pdf


26 We have analyzed over 400 cases out of which 94 cases have been used in this study. Refer to Chapter II: Methodology for more details.


28 The Recognize, Resist, Remedy project, supported by the International Development Research Centre (IDRC), Canada, is a research project aiming to combat gender-based hate speech against women in Brazil and India. See, Recognize, resist, remedy: Addressing gender-based hate speech in the online public sphere. (2020). IT for Change. https://itforchange.net/online-gender-based-hate-speech-women-girls-recognition-resist-remedy


35 Shreya Singhal v. Union of India, AIR 2015 SC 1523
38 Refer to Section 2.2.3 for more details.
57 Ibid.


Ibid.


Promoting enmity between different groups on grounds of religion, race, place of birth, residence, language, etc., and doing acts prejudicial to the maintenance of harmony.

Deliberate and malicious acts, intended to outrage religious feelings of any class by insulting its religion or religious beliefs.

Uttering, words, etc., with the deliberate intent to wound the religious feelings of any person.


Article 81A of the Criminal Code (Greece).


Council of Europe. (n.d.). *Combating sexist hate speech*. [https://rm.coe.int/1680651592](https://rm.coe.int/1680651592)


Multiple provisions have been used in a single case. This table has been generated based on reviewing provisions invoked in the cases shortlisted for this study, which are at different stages of the judicial process and often do not contain charging provisions.

The notion of modesty as a concern.

extend to two years, or with a fine, or with both.

outrage her modesty, shall be punished with imprison

or uses criminal force to any woman, intending to outrage or knowing it to be likely that he will thereby

91

which may extend to one year, or with fine, or with both.

intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term

modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending

90

years or with fine not exceeding two lakh rupees, or with both.

violating the privacy of that person, shall be punished wit

transmits the image of a private area of any person without his or her consent, under circumstances

where she would usually have the expectation of not being observed either by the

93

f_Digital_Technology%27s_Impact_on_Revenge_Porn

https://www.researchgate.net/publication/330401076_Nudes_are_Forever_Judicial_Interpretations_of_Digital_Technology%27s_Impact_on_Revenge_Porn

83


84

New South Wales Crimes Act, 1900. Section 91R. (Wales).


85


86


https://bridges.monash.edu/articles/journal_contribution/Regulating_the_Non-Consensual_Sharing_of_Intimate_Images_Revenge_Pornography_via_a_Civil_Penalty_Regime_A_Sex_Equality_Analysis/10279304?backTo=/collections/Volume_44_Issue_3/4732265

87


88


89

Punishment for violation of privacy: Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

90

Word, gesture or act intended to insult the modesty of a woman: Whoever, intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which may extend to one year, or with fine, or with both.

91

Voyeurism: Any man who watches, or captures the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator or disseminates such image shall be punished on first conviction with imprisonment of either description for a term which shall not be less than one year, but which may extend to three years, and shall also be liable to fine, and be punished on a second or subsequent conviction, with imprisonment of either description for a term which shall not be less than three years, but which may extend to seven years, and shall also be liable to fine.

92


93


94


https://doi.org/10.1177%2F1557085116654565

95


96


97

Assault or criminal force against a woman with the intent to outrage her modesty: Whoever assaults or uses criminal force to any woman, intending to outrage or knowing it to be likely that he will thereby outrage her modesty, shall be punished with imprisonment of either description for a term which may extend to two years, or with a fine, or with both.

98


The court also referred to culture, which has been discussed in the section on sexism (see section 2.4.5).

115 In criminal law cases, the burden of proof is expected to be “beyond reasonable doubt” of guilt of the accused. Criminal law. (n.d.). University of Minnesota. https://open.lib.umn.edu/criminallaw/chapter/2-4-the-burden-of-proof/

129 Nair, S. (2021). *How Tarun Tejpal was given access to the victim’s personal WhatsApp messages to build his defence*. NewsLaundry. [https://www.newslaundry.com/2021/06/09/how-tarun-tejpal-was-given-access-to-the-victims-personal-whatsapp-messages-to-build-his-defence](https://www.newslaundry.com/2021/06/09/how-tarun-tejpal-was-given-access-to-the-victims-personal-whatsapp-messages-to-build-his-defence)

130 Ibid.


142 A bailable offense is one which is shown as bailable in the First Schedule of the Code of Criminal Procedure, 1973, or which is made bailable by any other law in force. Bailable offenses are regarded as less grave and less serious. For bailable offenses, getting bail is a right and the accused can directly enforce this right. However, as a condition for release, the person needs to give security/money to the court, which assures the court that the accused will appear before the court whenever required and will not commit any crimes outside prison. The court usually fixes a standard threshold monetary amount to grant bail for various offenses. In some cases, where the accused does not have the bail money, the court may also grant bail based on a personal bond, which is a personal promise the accused makes. Non-bailable offenses are ones where bail is not a matter of right. For non-bailable offenses, getting bail depends on the discretion of the court. The possibility that a court will grant bail to the accused depends on various factors. The court considers gender, health, and age while granting bail.


Non-bailable offenses (committed against the body) include: murder (S. 302, IPC.) and dowry death (304 B); abetting the commission of suicide (S. 306, IPC) and attempt to murder (S. 307 IPC); attempt to commit suicide (S. 309, IPC); causing miscarriage without woman’s consent (S. 313, IPC); assault or criminal force to woman with intent to outrage her modesty (S. 354, IPC); kidnapping for ransom (S. 364A, IPC); rape (S. 376, IPC); gang rape (S. 376D, IPC); and unnatural offenses (S. 377, IPC).

144 All the conditions for bail in these cases are standard principles for it, set through judicial precedents over the years. This column highlights the unchanging nature of the conditions and how they are yet to address the online public sphere in the context of online violence. Refer to section 3.5.3.2 for further details.
The excerpts in this column are reasons, beyond legal ones, that have shaped the bail orders for perpetrators of online violence.


Satin, M. (2017). *Discretion, discrimination and the rule of law: Reforming rape sentencing in India*. Cambridge University Press. [https://doi.org/10.1017/CBO9781316471784](https://doi.org/10.1017/CBO9781316471784)


All the conditions for bail in these cases are standard principles for it, set through judicial precedents over the years. This column highlights the unchanging nature of the conditions and how they are yet to address the online public sphere in the context of online violence. Refer to 3.5.3.2 for further details.

The excerpts in this column are reasons, beyond legal ones, that have shaped the bail orders for perpetrators of online violence.


The power of a magistrate to grant bail in cases of non-bailable offenses is restricted if the offense is punishable with death or imprisonment for life.


Gudikanti Narasimhulu and Ors. v. Public Prosecutor, High Court of Andhra Pradesh, SCR (2) 371. (1978).


Digital misogyny as hate speech: Exploring legal implications, national dialogue on gender


189
its

#Gamergate'.

188
https://www.wired.com/2013/01/facebook

187
such content while protecting the identity of victims.

and social media platforms. During the course of hearings (in 2017), the Supreme Court direc

_initiated in 2015 in view of child pornography and rape videos being circulated on communication apps

Atlantic.

The State Of Madhya Pradesh

women for seeking redress.

to online trolling or harassment were received by the

A Press Information Bureau release indicated that from July 2016 to July 2017, 97 complaints relating

special

violence against women

Government of India.

183
182
181
180
179
178
177
176

175
Administrative Region.

174
173
172
171
170
169
168
167
166
165
164
163
162
161
160
159
158
157
156
155
154
153
152
151
150
149
148
147
146
145
144
143
142
141
140
139
138
137
136
135
134
133
132
131
130
129
128
127
126
125
124
123
122
121
120
119
118
117
116
115
114
113
112
111
110
109
108
107
106
105
104
103
102
101
100

(1978).


IT for Change. (2017). Submission on online violence against women to the special rapporteur on violence against women. https://itforchange.net/submission-on-online-violence-against-women-to-special-rapporteur-on-violence-against-women

A Press Information Bureau release indicated that from July 2016 to July 2017, 97 complaints relating to online trolling or harassment were received by the Ministry of Women and Child Development (WCD Ministry). While it is true that women do hesitate to register complaints or make public the sexual harassment they suffer (and in this case, those who did decide to complain may have also reached out to the local police), the complaints mechanisms of the WCD Ministry seem to be used by very few women for seeking redress.


190 Ibid.


https://static1.squarespace.com/static/58347d04beafbb1e66df84c/t/5d0074f67458550001c56af1/1560311033798/Facebook_India_Report_Equality_Labs.pdf


https://citizentruth.org/facebook-business-model-thrives-on-the-virality-of-hate/

197 Ibid.

198 Facebook admits it was used to ‘incite offline violence’ in Myanmar. (2018). BBC News.

199 Sreekumar v. v. State of Kerala, 2019 (2) KLT 642: 2019 (2) KLJ 832.


201 Ajit Mohan vs Legislative Assembly, NCT & Ors., W.P. (C) No.1088. (2020).

202 This was in response to the Notice for Appearance before the Delhi Legislative Assembly’s Committee on Peace and Harmony, NCT (National Capital Territory) of Delhi, dated 10 September 2020, where Facebook addressed the Chairman of the said committee. This communication, which has also been referenced in the Ajit Mohan judgment, openly disclosed Facebook’s removal of 22.5 million instances of hate speech content during the second quarter of 2020. This represented a significant increase compared to the meager 1.6 million instances removed during the last quarter of 2017.


204 The Present Petition Has Been … v. Unknown, Crl. O.P. No.12604. (2020).


208 The Present Petition Has Been … vs Unknown, Crl. O.P. No. 12604. (2020).


212 Latin for ‘friend of the court’; usually a lawyer who acts in an independent and neutral capacity to help the court with the case at hand.


215 Stern, R. (2016). Facebook is not neutral, UB privacy and social media expert says. UB Now.
http://www.buffalo.edu/ubnow/stories/2016/05/bartholomew-facebook-neutrality.html


221 In Re: Prajwala S.M.W. (Crl.) No. 3. (2015). and Sabu Mathew v. Union of India, W.P.(C) No. 341. (2008)., the Supreme Court broke away from this precedent by hauling up digital corporations such as Facebook, Twitter/X, Microsoft, etc., for failing to take action against the spread of rape videos and for allowing pretinal sex determinations on their platforms.

222 In 2017, Germany passed the Network Enforcement Act (Netzwerkdurchsetzungsgesetz, NetzDG) (also known as the ‘Facebook Act’). The law did not create any new duties for social media platforms but did impose high fines for noncompliance with existing legal obligations. The Act is applicable only to social media networks that have 2 million or more registered users in Germany. It obligates the covered social media networks to remove content that is “clearly illegal” within 24 hours after receiving a user complaint. If the illegality of the content is not obvious on its face, the social network has seven days to investigate and delete it. A social media network may be fined up to Euro 50 million (about USD 59.2 million) for noncompliance.


225 Chandrashekar, R. (2020). It’s time for India to regulate the internet and social media platforms. 
LiveMint. 


227 Proviso to Rule 4(2), The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021: Provided that an order shall only be passed for the purposes of prevention, detection, investigation, prosecution or punishment of an offense related to the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order, or of incitement to an offense relating to the above or in relation with rape, sexually explicit material or child sexual abuse material, punishable with imprisonment for a term of not less than five years.


245 These laws are expected to be overhauled with the introduction of new Bills – the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagrik Suraksha Sanhita, 2023, and the Bharatiya Sakshya Bill, 2023 – as of August 2023. However, comparative annotations show that large parts of the laws have remained the same, including verbiage around modesty.
249 Ibid.
250 Rai Sandeep @ Deepu v. State of NCT of Delhi, (2012) 8 SCC 21. The Supreme Court noted, “In our considered opinion, the ‘sterling witness’ should be of a very high quality and caliber whose version should, therefore, be unassailable. The Court considering the version of such witness should be in a position to accept it for its face value without any hesitation. To test the quality of such a witness, the status of the witness would be immaterial and what would be relevant is the truthfulness of the
statement made by such a witness. What would be more relevant would be the consistency of the statement right from the starting point till the end, namely, at the time when the witness makes the initial statement and ultimately before the Court. It should be natural and consistent with the case of the prosecution of the accused. There should not be any prevarication in the version of such a witness. The witness should be in a position to withstand the cross-examination of any length and strenuous it may be and under no circumstance should give room for any doubt as to the factum of the occurrence, the persons involved, as well as, the sequence of it."

253 Satish, M. (2017). *Discretion, discrimination and the rule of law: Reforming rape sentencing in India*. Cambridge University Press. [https://doi.org/10.1017/CBO9781316471784](https://doi.org/10.1017/CBO9781316471784)

252 Ibid.


262 The fiduciary relationship may arise in the context of a jural relationship or it may not. Where confidence is reposed by one in another, and that leads to a transaction in which there is a conflict of interest and duty in the person in whom such confidence is reposed, fiduciary relationship immediately springs into existence.”

As defined by the Madras High Court in the case: *Nellie Wapshare & Ors. v. Pierce Leslie & Co. Ltd. & Ors*, AIR 1960 Mad 410

265 Sexual assault by those who are related to the child by blood or in a position of power becomes aggravated sexual assault. See, *The Protection of Children from Sexual Offences Act* No. 32. SS. 5(n), 5(p), 9(n), 9(p). (2012). Government of India. [https://wcd.nic.in/sites/default/files/POCSO%20Act%2C%202012.pdf](https://wcd.nic.in/sites/default/files/POCSO%20Act%2C%202012.pdf)


268 Prashant Parashar v. The State Of Madhya Pradesh, M. Cr. C. No. 9720. (2017): About asking a 13-year-old to share nude pictures on social media;
Intimate

doesn't


https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3946893/

Malawi.

280 Tanzania: A cross sectional analysis. BMC Women's Health, 18(185).

https://itforchange.net/sites/default/files/1662/Born
digital, Born free? A socio-legal study on young women’s experiences of online violence in South India. IT for Change.


276 Rosco, J., & Lane, S. (2020). Statistical insights: EIGE’s intimate partner violence data collection. OECD.


278 Intimate partner violence.

https://apps.who.int/iris/bitstream/handle/10665/77432/WHO_RHR_12.36_eng.pdf;sequence=1


https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1831928/


https://www.researchgate.net/publication/313581719_Online_Shaming_and_the_Right_to_Privacy


https://www.researchgate.net/publication/353142525_Development_of_the_India_Patriarchy_Index_Validation_and_Testing_of_Temporal_and_Spatial_Patterning

277 Rosco, J., & Lane, S. (2020). Statistical insights: EIGE’s intimate partner violence data collection. OECD.


278 Intimate partner violence.

https://apps.who.int/iris/bitstream/handle/10665/77432/WHO_RHR_12.36_eng.pdf;sequence=1


https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7599123/


https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3946893/


Institutionalized hierarchies of cultural value that deny them the requisite standing.

Implementation of POCSO Act, 2012 for school management and staff.


in 2018, 117 cases of cybercrimes were committed against children and 79 such cases were registered.

These cases are related to sexual harassment at the workplace, wherein the perpetrator was hierarchically at a higher position than the victim.

These National Crime Records Bureau (NCRB) reveals a 400% jump in cybercrimes against children in India in 2020 from the previous year. In 2019, 164 cases of cybercrimes against children were reported while, in 2018, 117 cases of cybercrimes were committed against children and 79 such cases were registered in 2017.

Sexist and violent comments from social media users can have very real consequences for the individuals who are subject to them. In fact, it is often the case that these comments are made by people who are in positions of power over the individuals who are being harassed.

In this way, the use of social media platforms can be an example of institutional violence, where the institution is the internet platform itself.


IT for Change.
DOI:10.1080/0305764X.2014.987644

Indian copyright jurisdiction has seen several developments including introduction of John Doe orders for content takedown, as well as the more recent dynamic injunctions granted to Disney in order to block content that can re-emerge as a redirecting, mirror or alphanumeric website.

*See, India: Court issues first dynamic injunction.* (2020). Managing IP. 
https://www.managingip.com/article/b1kblk4hwfls04/india-court-issues-first-dynamic-injunction


New South Wales Crimes Act, (1900). Section 91R.