

Data, Gender, and Digital Harm: Rethinking Cyber-Crime Statistics on Women in India

*Mahera Imam,

Doctoral researcher at the Department of Women's Studies, Bharathidasan University, Tamil Nadu.

**Prof N. Manimekalai,

Head of the Department of Women's Studies, Bharathidasan University, Tamil Nadu.

***Prof S. Suba

Professor and Head in the Department of Women's Studies at Bharathidasan University, Tamil Nadu.

Abstract

How many women are included in the list of digital violence victims in India, and who does not count in our list? This paper challenges the cyber-crime statistics in India that are rapidly increasing with the help of a feminist, data-critical approach. The 2023 report of the NCRB on Crime in India indicates that despite the increase in the number of crimes being registered against women (approximately 4.5 lakh), overall cybercrimes increased by approximately 31 per cent in 2022-23 to 86,420 cases. Other legal studies on NCRB statistics approximate that approximately 28,903 of these cybercrimes were specifically categorised as crimes against women, falling under subsections on cyber-stalking, morphing, defamation and assault on modesty. However, international and regional surveys indicate that the range of technology-mediated gender-based violence (TF-GBV) is even broader: Economist Intelligence Unit research mentioned by the UN Women states that 38 per cent of women have experienced online violence in their personal lives, whereas a study of women journalists reports that approximately three-quarters of them have been targeted online. The paper is based on the idea that cyber-crime statistics are not neutral reflections of harm but infrastructural products of gendered infrastructures, reporting pathways and classification regimes, building upon the arguments of Safiya Noble on

the existence of the so-called algorithms of oppression and Ruha Benjamin on the so-called discriminatory design, as well as on Data Feminism of D'Ignazio and Klein.

In access to administrative data, however, there persists a mobile-internet gender gap, with women in low- and middle-income environments remaining nearly 15 per cent less likely than men to use mobile internet across the world and women merely 37 per cent of the global average using mobile internet on their mobiles, with a gap of about 30 percentage points between women and men. Marginalized women, such as rural, lower-caste, minority and youthful females, tend of all to file police complaints or resort to online grievance portals, which increases the silencing effect of statistics. Using the example of the Sulli Deals and Bulli Bai “auction app that was targeting Muslim women activists, journalists and students and recent cases of AI-morphed sexual extortion by predatory loan apps, the paper demonstrates that the harm of platform architectures, communal hate networks and data brokerage practices spill across legal categories (fraud, obscenity, defamation, stalking) while being counted as discrete incidents. It compares NCRB data to other sources of data on women on helplines or citizen-driven mapping projects such as Safe-city, Wikipedia and qualitative testimonies, conceptualising the notion of digital harm as cumulative, relational and labour-forming as opposed to episodic crime. The abstract therefore establishes three interventions namely, a critique of the ways in which the current categorizations of cyber-crime incite fragmented experiences of women in violence, an intersectional explanation of missing data achieved through digital divides and institutional prejudice, and a proposal to feminist indicators that redefine cyber-crime statistics as a kind of broader governance of data, platforms and safety. The paper argues that to make TF-GBV visible in SDG 5, digital-rights agendas and national strategies that purport to empower women by using data to govern women need to rethink cyber-crime statistics against women in India.

Keywords: Gender, Technology, Violence, Data, SDG, India

1. Introduction: Why Counting Cyber Violence Matters

Not only is the number of women victims of digital violence in India a question of fact, but it is also a question of governance: How many women count as victims of digital violence in India—and who remains invisible in our numbers? The state is what is measured and can be administratively seen, prioritised, financed, policed and regulated. Quantification scholars keep in mind that numbers are never descriptive: they are political tools that determine institutional focus and authorization. In this regard, crime measures are included in what James C. Scott terms the state endeavour to render social reality familiar, and Theodore Porter demonstrates how the numbers gain power precisely due to the way they seem objective and impersonal, although they are constructed based upon decisions regarding how to classify and how to proceed.

The consequences are particularly high in the case of technology-facilitated gender-based violence (TFGBV), since the digital harms are frequently disregarded as being virtual, interpersonal, or too diffuse to regulate until they can be quantified.

1.1 The main enigma: decreased official prevalence in the presence of greater measured prevalence.

This paper commences with an ongoing conflict: why are official cyber-crime statistics that relate to women victimisation seem to be comparatively low, despite surveys and industry research consistently indicating that women are frequently exposed to internet abuse and harassment? The UN Women has cited a study by Economist Intelligence Unit (EIU) in the world stating that 38 percent of women have personally endured online violence, and 85 percent have observed other women as victims of online violence. UN Women parallel Journalism On the same occasion, journalism, one of the occupations whose digital presence is inherently linked to work, demonstrates how ubiquitous and professionally chilling violence against women can be: A global survey conducted by UNESCO stated 73% of women journalists encountered online violence during their work. UNESCO These prevalence measures

make it clear how extensive the harm is, and yet they do not fit so easily into police categories, reporting channels, or record-keeping systems. India refracts this lack of fit in an especially acute way since it is

- (a) a large and fast digitalising society
- (b) a polity where cybercrime reporting structures are growing, and
- (c) a place where gendered inequalities around access, mobility, and institutional trust are being enacted.

As such, low numbers cannot be easily understood to mean low harm. They can also indicate the absence of connection, absence of reporting channels and absence of recognition.

1.2 What NCRB 2023 teaches us: expansion, intentions and location of sexual exploitation.

It is on this background that the Crime in India 2023 by NCRB is an indication of a sweeping change: the number of cybercrimes that are registered in the official statistics is increasing at a rapid pace. According to the NCRB report, the release, the overall number of cybercrime cases in 2023 is 86,420 cases (compared to 65,893 cases in 2022). Indian Express The same report states that the leading motive recorded is fraud (59,526 cases, 68.9 percent) with sexual exploitation (4.9 percent, 4,199 cases) and extortion (3.8 percent, 3,326 cases) coming second and third respectively. There are two points that are relevant to this paper. To begin with, the trend set by NCRB has proven that cyber offences are not marginal anymore, they are transforming the national crime profile. Second, even in the context of official frames, sexual exploitation is a separate category of motives, but it is not the only piece of gendered digital harms. There are numerous manifestations of TFGBV, including but not limited to doxxing, forceful outing, deep fake porn, stalking through technology, caste- and community-based hate drives, workplace trolling, and organized harassment that are frequently spread across legal categories and administrative platforms. This proliferation of scatter is important in that it influences what turns to

be visible as crime against women and what is internalized to other generalizations that may be cheating, defamation, obscenity, criminal intimidation, or IT Act offences.

1.3 There is high crime against women- but cyber harm can still be read partly.

The wider gendered violence catalogue of NCRB is not that small: in 2023, the release of the NCRB figures indicates a slight increase in the number of crimes against women to 4,48,211 (compared to 2022). New Indian express But this enormous universe of crimes against women does not directly connect with the cyber world, since the cyber layer is scattered in:

- committed cyber tables (such as the list of cybercrimes against women), and
- IPC/SLL categories in which the digital modality is never documented as the primary identifier, and
- harms mediated by platforms that do not even become FIRs (or become FIRs when worsened, recurrent, or catastrophic). That is, the very structure of the statistics, what is given a separate table, what is coded as motive, what is coded as method, what is not coded at all, becomes one of the primary subjects of analysis.

1.4 The structural nature of the visibility question: data are created, not discovered.

This paper thus does not consider the statistics of cyber-crime as such but as a social production, as it is constructed within the infrastructure, institutions and categories. In this case, feminist data scholarship is necessary. The Data Feminism by D'Ignazio and Klein predicts the infiltration of power into data with what is gathered, whose experiences matter, and whose experiences gain advantages in classification. The critique of algorithms of oppression by Safiya Noble and the work of Ruha Benjamin on discriminatory design goes further to demonstrate that digital systems unleash hierarchies not just in the behaviour of users but in its design, searchability, amplification, and differing protection. Just as significant are traditional lessons of the sciences and technology studies and sociology of classification the categories are not innocent. They fix some facts and destabilize others and, in both cases, much of the time in a manner that replicates institutional interests (such as the preference given

to discrete incidents rather than to cumulative harassment, or the preference given to a single-offence frame rather than a continuum-of-violence frame). It is the implication of this that this paper calls statistical silencing: individuals may be harmed, but they will not be counted because the harm is not unreal, but it is simply unrecorded in the books of accounts, not recorded in the records, or unacknowledged in the infrastructure.

1.5 The infrastructural hinge: the gendered digital divide as a problem of counting.

One of the key practices of missingness is the gendered digital divide, which is a reporting gap and an access gap. As an example, when discussing GSMA findings, it was mentioned that the level of women using mobile internet in India was 37 percent and the gender gap stood at about 30 percentage points. This is important as modern reporting channels such as a cybercrime portal, helpline, platform reporting interface, and digital evidence preservation usually presuppose stable connectivity, ability to access devices, privacy, and digital literacy. The women who will be most prone to laid vulnerability (rural women, lower-caste women, minority women, young women in precarious work, women under household surveillance) are usually at the same time those who will be least able to have the infrastructural conditions to transform harm into a formal complaint. Therefore, the enumeration of cyber violence is not a mere technical method of doing a better data. It is concerned with who is entitled to reach the state, who is able to safely record harm, who is able to bear the costs of complaint (time, travel, stigma, retaliation), and whether or not the institution is ready to acknowledge their experience as a cyber offence to begin with.

1.6 The importance of examples: between app auctions and AI-enhanced extortion.

The discrepancy between actual harm and law is manifested in symbolic cases. The Sulli Deals and Bulli Bai episodes can serve as an example of how the convergence of platform affordances, communal hate networks, and misogyny can result in very public, embarrassing, and targeted attacks, which outperform in terms of targeting Muslim women journalists, activists, and students in exceptional numbers. These occurrences do not always fit into one category of offence; they simultaneously

involve identity-related hate, sexual harassment, threats, defamation, data mining, and failure to control the platform. Similarly, the emergence of AI-assisted image editing and digitally mediated sexual extortion indicates a dynamic of harm that inflicts harm on victims and places them in the complicated system of remedies. These are not anecdotes which are added to statistics but indications as to why the statistics may be poor at describing harm: the unit of measurement (a discrete case) is not the same unit of experience (a cumulative campaign).

1.7 Paper Contribution: The cyber-crime statistics of women in India are not objective predictors of cyber harm.

They are created in the gendered disparities in access and safety, infrastructural digital disparities, reporting channels, and regimes of classification that fragment the experiences of women and make certain harms (and some groups) less visible than others.

The establishment of this introduction is three interventions that are developed within the rest of the paper:

- a critique of the ways in which current NCRB and legal categories might divide TFGBV into isolated, disjointed incidences,
- an intersectional explanation of missingness generated by digital inequalities and institutional prejudice, and
- a proposal of feminist indicators where digital harm occurs as cumulative, relational and governance-relevant.

1.8 Roadmap of the paper the paper follows the following procedure. Section 2 elucidates concepts and outlines TFGBV outside the confines of the limited understanding of cybercrime. To analyse how NCRB organizes cyberspace crimes, Section 3 looks at the cybercrime organization, the types of motives, those related to women, and legibility. Section 4 theorizes the so-called statistical silencing in terms of feminist data studies and classification scholarship, attributing it to reporting infrastructures and the gender digital divide. In Section 5, the author employs the

chosen case examples (such as auction apps and AI-enabled sexual extortion) to demonstrate spillages of harms across categories and why the cumulative harm frame is required. The section 6 suggests feminist indicators and complementary data sources (helplines, civil society mapping, survivor-centred documentation) to enhance measurement. The conclusion returns to the main argument: to render TFGBV governable, one needs to make it countable, however, counting itself has to be redesigned as a feminist project of recognition and justice.

2. Literature Review: Feminist Data Critiques and Cyber Violence

2.1 Technology-Facilitated Gender-Based Violence (TF-GBV): definitions, scope, and typologies

An emerging literature in international policy and studies does not regard technology-facilitated gender-based violence (TFGBV) as a novel form of violence, but as gendered violence re-structured using digital infrastructures. The novelty of misogyny in this framing is not necessarily the degree but rather the extent, pace, tenacity, findability, and reproducibility with regard to platforms and time with which networked systems facilitate the spread of abuse. This change in infrastructure is well understood in a widely-known definition of UNFPA in which TFGBV is defined as violence perpetrated, with the help of information and communication technologies and digital media, and at individuals on the basis of gender. More importantly, an online-offline continuum is also mentioned in TFGBV but not an autonomous virtual realm. UNFPA specifically states that such violence permeates into households and bedrooms, the workplace and the school, and may even start on the internet and become accrued offline (or the other way round), which supports feminist theory of the embodiment of mediated harm being experienced as fear, constraint, and risk management, and not as single-incident harm. The TFGBV lexicon currently has a wide and dynamic repertory: sextortion, image-based abuse, doxxing, cyberbullying, cyberstalking, online grooming, hacking, hate speech, impersonation, and tech-enabled monitoring or location tracking -forms which can intersect in bundles during targeted campaigns. United Nations Population Fund. Evidence on prevalence of

TFGBV through a world survey further underscores the fact that the vice is not peripheral. It was reported that 38 per cent of all women worldwide have been victimized online (by design and by region) in a synthesis prepared by ITU based on a study by the Economist Intelligence. Sector-specific surveys demonstrate even greater risk in professions involving interaction with the public: In the ICFJ global report on online violence against women journalists, 73% report having experienced online violence, with documented effects of this violence being threats, self-censorship, withdrawal of online interactions, and employment effects; it also reports a portion of offline violence being seeded online, demonstrating the continuum logic. There are two implications on the secondary-data paper concerning India. First, there is the issue of definitional scope: small categories of offences (e.g., cybers stalking) will underscore the experienced phenomenon when harms are multi-modal and cumulative. Second, prevalence estimates and administrative counts do not contradict one another they represent different regimes of measurement with different visibility thresholds, different denominators (internet users' total population), and different gatekeepers of recording (platforms, police, employer, family).

2.2 Feminist approaches to data and digital harm: why is data political? Feminist scholarship offers the conceptual framework to explain the discrepancy between the official figures and the daily prevalence. In various traditions intersectionality, feminist STS, critical race scholarship, and data justice each have made one common proposal: that data do not reflect the world in a way that is neutral, but are all the results of power-infused infrastructures (classifications, institutions, and norms) that condition what is legible as a case. Safiya Noble, in *Algorithms of Oppression*, and Ruha Benjamin, in her work about the discriminatory design provide a structural explanation of how hierarchies are reproduced by seemingly technical systems search, ranking, automated inference, and unequal distribution of harm. Their most important contribution to TFGBV Inquiry is to put emphasis on explaining not just by bad users but through a sociotechnical set-up that cries targeting profitable, frictionless, persistent (e.g., engagement-optimised recommender systems; virality; weak identity protections; and inconsistent moderation). This echoes the demands of UNFPA that

TFGBV does not lie in the realm of the so-called public spaces but deambulates through the commonplaces of work, intimacy and security. The approach of Data Feminism is more acute: missing data are not random occurrences but a systematic absence created by unequal distribution of resources, unequal credibility, and unequal access to measurement regimes (D'Ignazio and Klein 214). Missingness is frequently intersectional in TFGBV, with women and girls more vulnerable in terms of structure also likely to be least inclined to have access to a personal device, digital skills, designated reporting channels, or belief in institutional responsiveness, so their experiences are not statistically represented. This silence is further intensified whereby the measure requirement is based on formal complaint registration, formal platform reporting, or language/identity documentation, which is disproportionately not accessible. Quantifiers and classifiers in general (e.g., Bowker and Star; Porter) also contribute to understanding why cyber-violence is particularly vulnerable to being fragmented in numbers: classification systems are restrictive of boundaries (this is fraud, this is obscenity, this is defamation) when victims perceive cyber-violence as a sustained campaign. Even the EIU global prevalence project augurs such definitional and scaling decisions methodologically via a multinational survey and modelling corrections to approximate prevalence trends among nations, making it clear that prevalence is itself being constructed using an overt design of measurement. Lastly, the enabling conditions are addressed in the paper of Shoshana Zuboff: surveillance capitalism (and related political economy research) suggests that the extraction of data, prediction of behaviours, and the market of attention can establish incentive structures in which catering to targeted harassment is not a forgivable crime but a profitable one. Concisely: feminist digital theory does not accept cyber-violence statistics as a technical document but as a measure of whose harms are to be made governable -and whose harms are to be left out of the system classifications.

2.3 Indian context: measurement gaps (categories, reporting and digital gaps). The Indian system of crime measurement is pegged on administrative statistics of crime and legal types, most conspicuously, NCRB collections based on police files. Like other areas of crime, the reporting behaviour, policing style, local interpretation of the

law, and recording procedures are defining such datasets and not underlying prevalence. The crime statistics of Indian crime have long been constrained, research has pointed out, both by under-reporting and by inconsistent data quality across jurisdictions -constrains of its own that are inherent in administrative systems that rely on institutional registration as the state of visibility. PMC Legal fragmentation makes the problem of measurement critical in cyber-violence against women. The identical episode of abuse can be characterized by impersonation, threats, non-consenting sharing of images, extortion, casteist/communal slurs, and intimidation at work; but the administrative systems tend to record a single principal offence, or apportion aspects under the IPC and IT Acts, and conceals the campaign-like character of damage. Even in where reported on cyber-crimes against women, classification is prone to predetermine a narrow range of offence headings (e.g., cyber stalking/bullying; publishing/transmitting sexual content; related IPC provisions), which are prone to undercount newer and hybridised harms (coordinated hate networks, tech-enabled coercive control, and AI-enabled image-based abuse). This puts the digital divide in the form of a measurement divide. In the event of uneven access to the internet, smartphones and use of own device, the exposure, documentation capacity and reporting channels will be uneven as well. Evidence around the world demonstrates that gender gaps continue to exist in the area of connectivity: ITU states that in 2024 70 percent of men and 65 percent of women used the internet worldwide (and women continue to be a disproportional number of non-users), and gender balance is far to be reached in many places. Work by GSMA also reveals high disparities within LMICs in mobile-internet access, with women regarded as less likely to access mobile internet than men and, significantly, access to mobile internet due to various factors, such as affordability, skills, and safety/security, i.e., the very elements that determine whether a survivor can preserve evidence, navigate portals, or approach help safely. India-specific secondary reporting on the 2024 findings of GSMA show women are mobile internet users at approximately 37%, and there is a gender gap (still substantial but reported to narrow). Older but powerful survey data also records gendered disparities in smartphone ownership and urban

rural disparities, which supports the argument that, who can report is not morally arbitrary but socially stratified. Pew Research Center Combined, the numbers of Indian cyber-violence are to be read as institutional visibility figures: they indicate the point of contact between the harms of women and the state recording apparatus. A feminist data critique does not thus see low official numbers as an assurance, but as a diagnostic question: Which harms are inherently hard to name, to prove and to record, and which are women inherently least likely to be reflected in the record?

3. The Data Problem: The Underrepresentation of women in cyberspace Crimes statistics

A feminist data critique begins with a fundamental methodological assumption: the counts of NCRB cyber-crime are not prevalence measures. They are administrative production measures- output of a long pipeline where harm should be (i) felt, (ii) known wrong (iii) reported, (iv) registered as an FIR/ complaint, (vi) transferred into legal categories which are aggregate in NCRB. At each point in this pipeline, TFGBV is lost systematically. Not a random error, but systematic invisibility- what you are labeling statistical silencing.

3.1 Gendered access gaps: visibility as a prerequisite of connectivity. The initial breach of the pipeline is structural. Recounting cyber harm is progressively reliant on the access to a device, personal connectivity, and digital literacy, not only to navigate online spaces, but also to safeguard evidence (screen shots, URLs, metadata), locate platform reporting functionalities, and make use of state portals. The gendered connectivity gap between India and other countries is so big that it becomes a measurement issue by itself. According to secondary sources that report the findings of GSMA, the mobile internet users among women on their phone are approximately 37 percent and the gender gap between them and men is still wide. Complementary national and survey data Stratification by rurality and gender: a Yale EGC study reports that in its India setting 59 percent of rural women have access to a mobile phone compared to 80 percent of rural men (emphasizing that connectivity is not evenly distributed). Pew prior global surveys The existence of a sharp gender divide in

smartphone ownership in India (men 34, women 15% in 2018 survey data) was also documented by Economic Growth Center earlier Pew global survey evidence which indicated that access to smart devices generally (which are often needed to capture evidence and navigate portals), rather than universally, has been gendered. Pew Research Center Where having a phone appears to be high, even where access is usable, it is not necessarily private. NFHS-5 monitors women who use their own mobile phone, and even the headline bar is descriptive: the state has to measure the ability of women to use a phone by themselves, and it implicitly accepts restrictions such as sharing, limited use, and control. The practitioner-based evidence confirms the argument even further: According to a study brought out by Dvara Research, which interviewed low-income women across various states, access to mobile devices by women is frequently accompanied by unequal digital literacy in terms of advanced features the features necessary to secure reporting, manage their privacy, and document information. The implication of this on the counts of NCRB is that in case there is inequality in access, there is inequality in reporting capacity. The women who are most susceptible to layered vulnerability (low income, rural, socially marginalised, young) are also more prone to be digitally constrained thus their harms are less prone to cross the experience to formal complaint threshold.

3.2 Institutional obstacles to reporting: stigma, lack of trust and imbalanced capacity. Although women may be able to record harm, the second bottleneck is institutional: does the complaint turn into a registered case and is it treated. The mechanisms are specified through perception studies on policing. Status of Policing in India Report 2018 (Common Cause and Lokniti-CSDS) posed the question as to why women and young girls do not wish to approach the police. Fear of social stigma/harassment and abusive language by police was the most reported reason (19%), then the reasons of unsafe to women like the lack of policewomen, family limitations, and the challenge of repeated visits (18%). There were also systemic issues that were observed such as absence of FIR/complaint registration and absence of confidentiality. These are precisely the processes that feminist theory refers to as secondary victimisation: the costs of reporting may be social (shame), family (control

and reputation) and procedural (repeat visits, uncertainty, poor confidentiality), which have created predictable under-reporting. These barriers are multiplied by capacity and geography. There is no national infrastructure used to police cybercrime; it is spread over cyber police cells/ stations with considerable state difference amongst them. According to a Government of India PIB note, BPR&D is collecting state/UT-wise data on cybercrime police stations (as of 01.01.2022), and expressly says that states/UTs are establishing them, where and when it suits them- a polite way of saying that coverage is uneven. Press Information Bureau And even in case of units, forensic and investigative capability is a limiting factor; policy analysis of cyber forensics impetus in India points out growing investments as well as cautioning that the variations in capacity might impede investigative efforts in the nation. Orf Online Lastly, the issue does not lie in the existence of cases being filed or not; but in the manner in which they are coded when they are. The two categories of fraud are the administrative leadership forms of cybercrime, with sexual exploitation showing as a smaller percentage share recorded by NCRB itself with the 2023 framing of the subject matter. In fact, at times, TFGBV incidents cross between the categories of offence harassment connected with impersonation, extortion, intimidation, so-called defamation, or so-called obscenity, financial fraud, or not-gendered headings. What results is misclassification or de-gendering: what is experienced as gendered in the world seems, in statistics, gender-neutral.

3.3 Infrastructural and platform biases: where design amplifies the bad and dilutes responsibility. Feminist political economy perspective demands undercounting cannot only be a problematic issue of police. It is also a governance issue of platforms - since platforms define (a) the scale of harassment, as well as

(b) the visibility of harassment to the systems of moderation.

(i) Weak pathways of grievance and evidence. The national reporting infrastructure of India has a specific route where one can report crime related to women/child using the National Cyber Crime Reporting Portal, that there is a portal: but what of the structural burdens mentioned above: the complainant must still have certain access,

access that is stable, as well as evidence, and procedural competence and confidence that he/she is not going to be shot in the back.

(ii) Asymmetry of language and moderation. One of the India-specific aspects is that abuse and hate tend to spread in the regional languages and code-switches, whereas moderation tooling and reviewer capacity were traditionally weaker-non-English. In the 2021 whistleblower cycle, the news of internal document reporting revealed that there were worries about insufficient resources to conduct reviews and content detection of important Indian languages such as Hindi and Bengali. The technical challenge is brought into focus by the Research and policy discussion on the topic of low-resource languages: detecting abusive content in Indic language and mixed-language (code-switched/transliterated) text is a research problem under active investigation, which can also explain the inconsistent and slow enforcement. In the event of moderation failure in regional languages, particularly among targeted populations such as women in the vernacular publics, the target population is overexposed and under protected.

(iii) Architecture, which is viral-able and pile-on. Coordinated harassment coordinated scaling In platform design, recommender systems, resharing mechanics, quote-posting, trending, and engagement-optimised amplification can facilitate coordinated harassment and rapid scaling. An analysis of platform design and algorithm management of polarization/violence by Knight-Columbia explicitly explains how design can facilitate mass manipulation and harassment and how the governance needs to think about these pathways of structure. Knight First Amendment Institute Critical scholarship also claims that toxicity is an attribute of a user, but can be angry intentionally, conditioned by technical architectures and incentive schemes. nature.com Why this is significant to NCRB numbers platform architectures are capable of generating high-frequency, high-volume harassment, which may be felt as cumulative (weeks/months of attacks, threats, impersonation, doxxing) but cannot be easily rendered into a single clean offence record. The politics of counting confronts architecture of harm.

3.4 The argument of statistical silencing: the theory of intersectionality as a theory of missingness.

Combining these fragments produces the very argument the most exposed folks to TFGBV tend to be the least represented in the official cyber-crime statistics. This is measurement intersectionality. Under-reporting of harm is experienced when gender disadvantage is combined with digital disadvantage, family control, stigma and institutional distrust. Where vulnerability enters into language marginality and weak moderation damage is more apt- but in a less controllable way, by the normal channels of complaint. And where vulnerability is combined with targeting on a political and communal level, harassment becomes organized and bullying-like in nature- usually resulting not in reporting but in self-censorship. The idea of independent monitoring highlights the fact that the online abuse in India is disproportionately applied to journalists, activists, and marginalised groups. To illustrate this, Freedom House reports that in India, internet users, such as journalists, activists, and representatives of the marginalized groups, have been the frequent targets of hate speech and being harassed on the internet. Freedom House When the targets of the greatest concern are the greatest cost reporters (social backlash, doxxing threats, occupational consequences, naming and shaming), then missing data recapitulate marginalisation. Then statistical silencing is not a figure of speech. It is a theory of data system and institutional and infrastructural interaction creating patterned absences: Silencing of access (no personal device / low connectivity / low skills)

- Silencing in the institution (stigma, fear, lack of confidentiality, weak registration)
- Classification Silencing (TFGBV coded as fraud/obscenity/defamation; harm fragmented among headings)
- Platform silencing (weak language moderation and irregular remedy)

Introduction to the next section: this diagnosis preconditions why the paper has to (a) compare NCRB data with other sources (helplines, civil society reporting, qualitative

testimonies), and (b) suggest feminist indicators that consider TFGBV a cumulative, relational, and structurally produced phenomenon (not only as episodic cases).

4. Case Illustrations: When Harm Exceeds Classification

These examples are not anecdotal add-ons to trends in NCRB; they demonstrate why administrative categories fail to describe TFGBV on a regular basis. In all instances, the pattern of analysis is similar: (i) the harm is multi-modal and cumulative, (ii) the legal/administrative system tends to only recognize discrete and countable incidents, and (iii) the fact that the platform is designed in a way that amplifies abuse and makes it more difficult to categorize.

4.1 The Sulli Deals and Bulli Bai applications: the communalised misogyny which falls out of one box of offence.

Harm can be irretrievably tied to religion, the public speech, and planned hate as seen in the episodes of the auction app. Reuters also had a report that police arrested a suspected author of an app that posted pictures of Muslim women in an act of virtual auction, which existed on GitHub and used an offensive word, and was removed. Reuters Al Jazeera also reported the event to have sold over 100 Muslim women highlighting the magnitude and the fact that there was a community target. Issue of classification: as indicated by charge-sheeting presented in the press of India, the legal response is necessarily scattered over a number of provisions- e.g. IPC provisions on promoting enmity/disharmony and sexual harassment/insult to modesty, and IT Act sections. In an article on the Delhi Police charge sheets, Business Standard specifically mentions a certain section of the IPC 153A/153B/354A(3) and the sections of IT Act 66/67 (according to the police sources). Business Standard But the harm that has been experienced outstrips these headings: • sexual harassment (objectification, humiliating), • religion-based hate (communal vilification, minorities against minorities), • data exploitation (non-consensual use of images and identifiers), • political intimidation (most of the victims were journalists/activists), and • a chilling

effect of speech and participation. This is direct in terms of civil liberties framing: the Internet Freedom Foundation described such incidences as the violation of privacy, dignity, and free speech, rights not readily superimposed by traditional offence-taxonomies. The most important thing to note in your paper is methodological, which is that it cannot be seen as a communal-gendered assembly of harm using NCRB-style counting, because it has to count it as a number of individual, countable offences- or only a number of lead offenders.

4.2 Deepfake and morphing scandals: AI-permitted abuse defeats old crime codes.

Cases of Deepfakes and morphing illustrate a second way of undercounting: new modalities, which were not invented by the old codes to refer to. The loan-app extortion trend is particularly educative as it superimposes financial fraud and sexualised pressure. India Today carried the claims that loan apps were transforming images of women (associated with deepfake abuse) in extortion schemes. India Today Newer coverage indicates the same trick as an operationised scam model. Individually, an article by the Times of India (Hyderabad) talks about a woman being blackmailed after fraudsters had made morphed pornographic videos of her face, increasing the pressure to avoid spreading it. A similar incidence of blackmail/extortion through morphed pornographic videos is carried in The Times of India The New Indian Expression. The New Indian Express Classification problem: these cases are frequently categorised into two or more legal buckets simultaneously, e.g. fraud/cheating/extortion and image-based sexual abuse and threats and digital impersonation, i.e., the gendered and sexualised coercion may be lost within the statistics of the fraud-heavy category of cybercrime. This ties directly to the trend of NCRB in which cybercrime is administratively overshadowed by motives of fraud, with TFGBV-reliant harms as a minor apparent percentage. Another implication (which would be helpful in your argument): AI-driven image abuse creates repeatability and permanence, i.e. content may now be reposted, re-edited and re-contextualised so the unit of harm is not a single incident, but a persistent exposure risk. This chilling effect is observed in a recent article by the Guardian about nudify tools and the AI deepfakes

when it comes to Indian women who post less and engage less out of fear of victimization with a manipulated image.

4.3 Women journalists and political leaders harassment: when it is occupation governance. TFGBV acts as an informal regime of labour control to public-facing women, such as journalists, politicians, activists: it regulates what they can say, be seen, and be involved in. According to a survey conducted by UNESCO (carried out together with ICFJ), 73% of female journalists surveyed had encountered online violence during their work with significant percentages of the surveyed reporting being threatened by physical and sexual violence. A further behavioural consequence is documented in the synthesis of the findings by UNESCO ICFJ, where a large proportion of report self-censorship and withdrawal online engagement, giving a picture of how online violence defines professional practice and public presence. The International Center of Journalists. Classification issue: a lot of this online violence is cross-platform and repetitive (pile-ons, coordinated trolling, threats, doxxing, impersonation), but administrative data systems are likely to document the case as a single offence (when documented at all). On a macro level, Freedom House also reports that Indian users of the internet such as journalists, activists, users of marginalized groups are also falling victims of online harassment and hate speech. Freedom House The analytical perspective of your paper: TFGBV in this case is not actually a crime event but a technology of government that organizes who can safely conduct themselves in the public.

4.4 Crowdsourced websites as alternative data: bringing patterns to sight beyond FIR-based measurement.

Since formal statistics are pre-disposed by the registration/reporting, alternative sources of data are vital in observing what NCRB systems do not detect, such as the so-called lower-intensity but high-frequency harassment that women have learnt to live with or tolerate without involving the police. Safecity, in particular (Red Dot Foundation), openly crowdsources anonymized stories about sexual harassment/abuse and maps them as hotspots to show local tendencies and trends

- and includes experiences that never get to be FIRs. SafeCity Plan international (Free to Be Delhi city report) makes a series of crowd-map with anonymity inviting girls and young women to designate unsafe/safe areas, explicitly mentioning anonymity as an incentive to participation and disclosure.

Safetipin (2017) implements a crowd-sourced safety audit model and generates mapped safety scores and heatmaps, which demonstrate how participatory civic data may be used alongside the official crime rates. Why this supports your argument: such efforts indicate that measurement itself is a politics of visibility. In NCRB, which relies on institutional registration (high-threshold pathway), every day, cumulative harms (lower-threshold pathway) can be documented by crowd-mapping tools. When combined, they justify the assertion by the paper that it is not accidental that data are missing; it is the structural result, that it needs the design of indicators that are feminist and triangulation of the multiple sources, rather than just more policing.

5. Thinking over Digital Harm: Feminist Analytical Framework (Structural–Infrastructural-Institutional).

The current paper presents an argument that cyber-crime statistics of women is not a clear window into TFGBV. They are the product of three inter-relating layers whether harm may pass through experience → evidence → complaint → registration → classification counting. The injury is statistically insignificant, when any of the layers closes that route of action.

5.1 The model (three dimensions) Consider TFGBV presence as generated by a triangle: 1. Structural level (accessibility and resistance to damage/reporting) 2. Infrastructural layer (how platforms/AI systems scale and form damage) 3. Institutional layer (the way the state documents, identifies and categorizes harm) Collectively these layers form (i) what is seen (ii) what is unseen, and (iii) what cannot be enumerated.

(A) STRUCTURAL: Inequality as a measurement issue. This is built on the feminist intersectional scholarship (Crenshaw): gendered harm is structured by caste, class,

religion, region, age, sexuality- and equally data visibility. When there is an unequal access, privacy, literacy, and social permission, then the counting of people is inequital.

A1. Digital divide = reporting divide. GSMA latest analysis of LMICs reveals that women are 15 percent less likely to use mobile internet as compared to men. GSMA In India, the secondary coverage of GSMA results states that there were approximately 37% of women who use mobile internet and the gender gap was significant (reported to have been narrowing but significant). ETGovernment.com Why this is important to counting: contemporary reporting means access to devices + constant internet availability + privacy + recording. In case of such unevenness, the dataset is not missing at random. It has been lost on the social axis-generating statistical silencing.

A2. Crossings enhance invisibility. The model considers undercounting structural: access and vulnerability to social risk, especially of young women, Dalit/Adivasi women, Muslim women, queer persons; and women subject to household surveillance are the least able to: • document harassment safely, • retaliate not by keeping digital evidence, • go up to police and treat them without stigma, • endure by a protracted complaint procedure. So few numbers can imply much friction, not much harm.

(B) INFRASTRUCTURAL: Platform/AI design as a harm multiplier (and a counting disruptor). The infrastructural layer asks: what is easy on platforms (virality, impersonation, pile-ons) and what is hard (rapid remedy, accountability, traceability)? It is based on the critiques of Noble and Benjamin, as well as data-feminist critiques.

B1. Incidents are transformed into campaigns with amplification systems. Resources facilitate harassment by scaling up via resharing, trending, recommendation, and networked pile-ons, so the unit of harm experienced is often cumulative (days/weeks/months) as opposed to a single event. Administrative datasets, in turn, lean towards discrete units ("case/FIR/section) and develop an incongruity between data shape and harm shape.

B2. A machine-learned type of abuse evades category. AI-morphing/deepfake abuse shows how rapidly the modality of harm is changing, which is higher than crime codes and recording practices. One recent report of a case in Hyderabad indicates that it was an extortion through morphed pornographic videos, and (critically) it quotes a pattern of cases at the state level: 23 cases of morphed obscene videos, 223 cases of doctored photos reported between April and October 2025 (according to the Telangana Cyber Security Bureau quoted in the report). The Times of India Counting: These cases frequently fall under fraud/extortion, and/or (abortion) IT Acts categories, although the gendered sexual-coercion aspect has been eroded or watered down, particularly in a cybercrime universe where NCRB demonstrates that fraud is top on the recorded motive list. The Indian Express

(C) INSTITUTIONAL: The policing, law, and classification as the gatekeepers of visibility. Though women have access (A) and harms are extreme (B), the institution layer determines whether or not the harm is a record, and what the record will be.

C1. Stigma and distrust are the contributors to reporting. According to the Lokniti-CSDS/Common Cause Status of Policing in India Report 2018, the most common reason women do not approach the police is that they fear social stigma/harassment and abusive language by police (19%), followed by the reasons women do not approach the police because it is unsafe (16-27) and because of the system (including FIR registration and the secrecy of information). This is textbook logic of secondary victimisation in that reporting may become expensive to survivors in a rational way.

C2. TFGBV is discontinuous in legal taxonomies. NCRB is a combination of classifications in both IPC/IT Act, whereas TFGBV periodically crosses buckets (threats + stalking + impersonation + hate speech + extortion + image-based abuse). This promotes misclassifying (e.g. into obscenity/defamation/fraud) and de-gendering (gendered harm being registered as gender-neutral offence).

C3. There are portals, and there is small equity. India has a specific National Cyber Crime Reporting Portal and channel of Women/Children related crime. Cyber Crime India+1 However, the existence of the portal does not address the structural barriers

(A), and the trust/friction barriers (C1). It is even capable of pushing the burden on to survivors: they have to be aware of the procedures, keep the evidence intact, and manage follow-ups.

5.2 What the model describes: Visible / Hidden / Uncountable What comes into sight (high probability of entering NCRB-type counts) • Heavy cybercrime by fraudsters (high reporting, better trace trail, faster routinisation by police). The NCRB 2023 reporting demonstrates that fraud is highly-run motive in cybercrime. • TFGBV which are similar to well-known templates (clear stalking cases, clear image circulation with recognizable accused, clear extortion) What is concealed (experienced, but sieved out before registration) • Common harassment (trolling, sexualised remarks, intimidation) that women either cope with through blocking, self-censorship or withdrawal. • Hamas evidence that is difficult to maintain (ephemeral material, numerous witnesses, anonymous networks). • Hamas in vernacular/coded speech in the circumstances when the platform enforcement is not always the same and the remedy is slower and more difficult to document. What cannot be counted well (even though incidents might seem to appear). • Compensatory damages: psychological distress, tarnished reputation, impeded mobility, forfeited career prospects, self-censorship. - Campaigns across platforms/time (a months-long pile-on can not be represented by a single case). • Intersectional targeting (gender + religion/caste) wherein the dimension of hate and sexual harassment are divided into different legal boxes. The framework can be summarised as follows: TFGBV can be statistically visible only with (A) access, (B) platforms leave legible traces and do not overwhelm victims with scale and (C) institutions are registering and coding the harm as gendered cyber violence instead of spreading it out across categories.

6. Bringing back the Data: What ought cyber-Crime Statistics to Reflect? There is no concept of cyber-violence versus women in the vacuum. It is not merely a gap in the reporting that is causing it to be underrepresented in crime statistics, but it is a crisis of data imagination. According to feminist researchers like D'Ignazio and Klein (2020), the nature and content of what we choose to measure, and how, is always influenced by power. Therefore, data justice TFGBV should go beyond the reactive crime statistics

and construct a plural, feminist, and intersectional measurement ecosystem with the survivors at the core.

6.1 NCRB Extensions: Triangulation of Better Indicators. (i) **Victimisation Surveys:** The Measurement of Experience and not registration. Customary crime statistics such as that of the NCRB capture registered not experienced harm. The concept of victimisation surveys has been circulated to reveal the dark figure of crime, which are the cases that go undocumented or are wrongly categorised as such by feminist criminology. The Violence Against Women Instrument (WHO) and the EU Agency of Fundamental Rights surveys have offered a detailed insight into technology-mediated abuse internationally especially in younger women, journalists, and politically active users. Surveys that measure: It can be described by exposure to various types of TFGBV (e.g. stalking, impersonation, deepfake abuse). • Digital abuse frequency/recurrence. • Repercussions (mental health, withdrawal of work, censorship on oneself) • (ii) **Intersectional vulnerabilities** (age, caste, religion, profession). would give a more grounded picture of prevalence of TFGBV in India, compared to what NCRB data would offer. **Introduction:** The concept of platform-level transparency report represents a fresh emergence that is approaching the stage of maturity **Background:** **Platform-level Transparency Report: Using Private Data to Do Good.** Such platforms as Meta and Twitter/X publish transparency reports, which list enforcement measures against harmful content, such as harassment, nudity, and hate speech. Nevertheless, according to scholars (Gillespie, 2018; Suzor, 2019), such reports are usually selective, non-standardised, and do not give disaggregated data on gender or region. **Platform data needs to:** • Disaggregated by gender, geography and language. • Monitor repeat criminals, networked harassment, and report resolution. • Not only self-published, but audited. India would impose requirements to disclose data on TFGBV on large platforms through IT Rules 2021 and through future Digital India Act. (iii) **Civil Society and Helpline Data: Getting Invisible Harms.** Such NGOs as Safecity, Aman Network, Point of View, and Breakthrough gather data by way of helplines, citizen mapping, and survivor testimonies. These records capture: Low-intensity and high-frequency damages. • Cases that survivors do not want to report to the police. Trends in the

regional languages or offline to online patterns of abuse. Such datasets are important especially to demonstrate normative, internalised, and non-reportable digital violence (e.g. everyday verbal sexual harassment, slut-shaming, casteist abuse). They play a decisive default to both NCRB and platform data.

6.3 The Intersectional Data Requirement: Visibleness of Marginalisation. TFGBV does not occur uniformly. Dalit, Adivasi, Muslim, queer, and disabled women experience multiple vulnerabilities simultaneously- however, the Indian statistical apparatus is not prepared to address identity-specific digital violence. The significance of intersectionality to TFGBV measurement: • Caste slurs, sexual violence threats and humiliation tricks are not reported or taken seriously in the systems of cybercrime. Communal targeting (as in Sulli Deals and Bulli Bai cases) is divided into two parts on the subject of obscenity and communal hate, making the gendered logic obscure. Queer and trans people who are usually outed or doxxed become the victims of the heteronormative legal systems. Identifying as disabled women increases their reliance on digital technologies to work and be connected, which makes TFGBV effects more isolating and less visible. A framework of feminist indicators should clearly disaggregate data according to caste, religion, disability, sexual orientation, region, and age, in connection with global demands of inclusive gender data (UN Women 2023; ITU Gender Digital Divide reports).

6.3. Towards a Feminist Data Governance Model. Feminist data governance does not only concern gathering datum better. It is concerned with redefining the notion of data, the epistemic authority, and the redistribution of power within the data pipeline. Based on the seven pillars of Data Feminism (D'Ignazio and Klein, 2020), the following pillars should be suggested to measure TFGBV:

Principle	Implication for TFGBV Data
Examine power	Ask who defines cybercrime categories; whose experiences are normalised or ignored

Elevate emotion and embodiment	Recognise trauma, fear, shame, and self-censorship as measurable impacts
Rethink binaries	Move beyond “victim/perpetrator,” “online/offline,” and “public/private”
Challenge default classification systems	Treat NCRB coding (e.g., “defamation,” “obscenity”) as contingent, not fixed
Embrace pluralism	Use survivor-led research, feminist helpline data, and participatory mapping
Make labor visible	Count emotional labour, tech navigation, and self-protection as part of harm
Take action	Design data systems to inform intervention—not just documentation

6.4 Legal and Policy Shifts Needed: From Reactive to Responsive Governance

(i) India’s Digital Personal Data Protection Act (DPDP Act, 2023)

While the DPDP Act focuses on consent and personal data processing, it has implications for image-based abuse, doxxing, and unauthorised profiling. However, it lacks a gender lens and clarity on enforcement in cases of TFGBV. Feminist digital rights scholars (like Usha Ramanathan and Malavika Jayaram) have warned that without intersectional harm framing, privacy laws may fail survivors.

Recommendations:

- Recognise intimate image abuse and deepfake harms as data rights violations.
- Provide survivor-friendly grievance mechanisms under the Act.
- Align with global principles (e.g., UN Cybercrime Convention draft, 2024).

(ii) Updating IT Act & NCRB Classifications

- Add specific TFGBV offences like deepfake dissemination, sexualised trolling, and impersonation.

- Allow multi-code registration of cybercrime incidents across categories (not just “principal offence”).
- Train police and cyber cells in recognising intersectional, cumulative TFGBV, especially in non-English and regional contexts.

(iii) Strengthening Cyber Cells and Reporting Infrastructure

- Universalise women-friendly cyber cells across districts.
- Build multilingual, accessible, and survivor-centred online reporting systems.
- Integrate NCRB systems with helpline and platform data for cross-verification and trend analysis.

Concluding Transition:

The reconstruction of cybercrime statistics must begin with a conceptual shift—from counting “cases” to accounting for power, harm, and exclusion. To make TFGBV visible, measurable, and governable, India must adopt intersectional, feminist, and survivor-centred data practices. Not only will this fulfil the spirit of SDG 5 (gender equality) and SDG 16 (justice and accountability), but it will also reshape how we imagine safety, participation, and justice in the digital age.

7. Discussion

7.1 What Does the State of Underreported Numbers Imply to the Digital Citizenship of Women?

This paper focuses on how digital harm is caused by digital platforms and how it diminishes the rights of women as citizens. Cyber violence is not only a technological issue, but it is a political issue. Under-recognised, under-reported and under-counted TFGBV has a direct impact on undermining women right to safety, dignity, participation and justice in the digital age. According to female theorists (e.g., Nancy Fraser, Nussbaum, and Crenshaw), the triadic issues of recognition, redistribution, and representation have long been regarded as the main elements of democratic inclusion. Digital platforms are now playing a critical role of visibility, labour, education,

mobility, and voice, yet TFGBV actively causes women to relegate to the peripheries of digital spaces. In that regard, underreported statistics do not merely comprise the lack of data, but rather, a mirror of failures in the architecture of securing the digital citizenship of women. A right to express, mobilise, work, and engage online is defected when abuse becomes a standard, solutions to abuse are not available and the harm is not rewarded by the state.

7.2 Effects of Silencing: Exposure to Withdrawal. One of the main themes of the global studies is the concept of the silencing effect of cyber violence. According to the global study by UNESCO and ICFJ of women journalists, the most prevalent reaction to persistent abuse on the Internet is self-censorship. Female journalists and newspaper reporters among the Indian respondents said that they have a systematic approach to commenting on political or gender related matters and posting tweets and even quitting platforms. Equally, qualitative research by organisations such as Point of View and IT for Change indicates how women with disadvantaged origins, especially those who are queer, Dalit women and Muslim women, abdicate online interactions because of the fear of coordinated assaults, doxxing, and sexualised threats. It is not merely an individual reaction but a compelled withdrawal out of the world. The major consequences of TFGBV are self-censorship and withdrawal to digital space which NCRB statistics do not record. Through the loss of agency when a woman opts not to make a post, or speak, or campaign, or express herself, in case of a backlash, it is an intangible loss of agency that statistics cannot track, but which redefines the parameters of the communal discourse and democratic engagement.

7.3 Labour, Mobility and Political Participation. The effects of TFGBV have a long way beyond the screen. Online abuse is a very real professional blow to women in the workforce: in media, education, IT, gig platforms and politics. • Lost opportunities: invitations to speak, write in public, leadership positions were refused in the fear of Internet threats. • Distorted career directions: others change directions or abandon platforms altogether. • Loss of mobility: after the episodes of TFGBV, the young women in conservative families feel more restricted. Casteist and misogynistic abuse is regularly directed at women political leaders, and in particular at those representing

marginalised groups (e.g. Dalit or Muslim women MLAs or councillors). A report commissioned by Association of Democratic Reforms (ADR) and freedom house points to online abuse as an implication that can discourage women to venture into political life particularly in an electoral environment. Effectually, TFGBV acts as a type of informal state of gender regulating who is allowed to be visible, credible, and influential in the digital life aspect of publicity.

7.4 SDG 5 and SDG 16 Accountability and Gender Equality link. Digital harm has been specifically identified by the Sustainable Development Goals (SDGs) as an impediment to equality and justice. • SDG 5.2 requires the eradication of any types of violence against women both in the physical and virtual environment. 5.b SDG aims at improving the access to empowering technologies in order to empower women. • SDG 16.3 encourages equal access to justice by everyone and includes the functionality of redress systems to cyber harm, as well as their fairness and survivor-centredness. • SDG 16.10 facilitates access to information and safeguarding of inalienable freedoms both of which are undermined when women self-censor or withdraw because of TFGBV. The underreported figures of cybercrime against women in India is a blind spot on national accountability as well as the global SDG monitoring. In the absence of a reconceptualization of the meaning of data, indicators of progress will be used as an authorisation of superficial reforms and concealment of institutional exclusions.

7.5 Underrepresentation to Epistemic Injustice. Lastly, when TFGBV is undercounted, it is not just a policy failure but it is actually an example of epistemic injustice (Fricker, 2007). Failure to believe, classify, and even record women digital harms means not only that they will not be included in the data, but also that they will not have the right to determine their own experience. The politicizing of harm through naming, recording, and counting is feminist. It determines who has their suffering rendered visible to the state, who is resourced in security and who is heard in the digital public.

Domain	Consequence of Underreporting
Labour	Loss of income, mobility, career visibility
Politics	Deterrence from public expression and leadership

Expression	Silencing, self-censorship, fear of visibility
Data Governance	Misaligned indicators, gender-blind policy responses
Justice Access	Survivors excluded from formal redress systems

Cyber violence is not just an individual violation—it is a collective democratic deficit. Making women’s digital harm visible, measurable, and governable is central to building an inclusive, accountable, and participatory digital society.

8. Conclusion: Toward Visibility, Justice, and Safer Digital Futures

This paper has critically interrogated the landscape of cybercrime statistics on women in India through a feminist, data-justice lens. Drawing from global prevalence reports, NCRB crime data, platform abuse patterns, and illustrative case studies such as the *Sulli Deals*, deepfake extortion, and harassment of women journalists, it has demonstrated that cyber-violence is structurally underreported, systematically misclassified, and epistemically silenced.

Despite the sharp rise in recorded cybercrime cases in India (86,420 in 2023), the forms and frequencies of technology-facilitated gender-based violence (TFGBV) remain partially visible in administrative data. This invisibility is not accidental—it is shaped by gendered access gaps, infrastructural bias in platforms, and institutional barriers to reporting and recognition. Women from marginalised caste, religious, linguistic, and gender-diverse communities are especially vulnerable to such erasures.

At the heart of this paper lies a simple but radical proposition: counting is a political act. As D’Ignazio and Klein (2020) argue, numbers do not merely reflect the world—they construct it. The way we define, register, and aggregate cybercrime shapes which harms are rendered governable, which bodies are deemed protectable, and whose safety counts.

To make digital spaces genuinely inclusive and just, we must move beyond narrow criminal-legal framings and adopt feminist, intersectional, and multi-source frameworks for data governance. This includes:

- Designing victimisation surveys for TFGBV,
- Triangulating NCRB data with platform reports, helpline records, and civil society mappings,
- Disaggregating data by caste, religion, sexuality, disability, and region, and
- Challenging default classification systems that fragment and de-gender women's experiences.

At the policy level, this demands two concurrent transformations:

1. **Fixing data governance:** updating IT Act provisions, ensuring accountability in platform transparency, and building survivor-centric digital complaint infrastructures.
2. **Addressing structural inequalities:** closing the digital gender gap, strengthening access to justice for marginalised women, and ensuring intersectional digital rights in national strategy and SDG monitoring.

In sum, building safer digital futures is not just about moderating content or expanding cyber cells. It is about transforming the structures of visibility, power, and participation that define women's digital citizenship. Until data systems can recognise all women in their full diversity and all harms in their cumulative complexity there can be no true justice in the digital public sphere.

Acknowledgement

I am deeply honoured to have been awarded a Doctoral Fellowship by the Indian Council of Social Science Research (ICSSR). This publication is an outcome of ICSSR-sponsored doctoral research. However, I bear sole responsibility for the information presented, the views expressed, and the findings of this study. I am sincerely grateful to the ICSSR, Ministry of Education, Government of India, New Delhi, for their invaluable financial support, which made this work possible.

**Research Scholar, Department of Women's Studies, Khajamalai Campus, Bharathidasan University, Tiruchirappalli, 620023, Contact Details: 9625614655, maheraimam8@gmail.com*

**** Director And Head (Retd), Department of Women's Studies, Khajamalai Campus, Bharathidasan University, Tiruchirappalli – 620023, Tamil Nadu, India**

***** Professor, Department of Women's Studies, Khajamalai Campus, Bharathidasan University, Tiruchirappalli- 620023.**

References

- Benjamin, R. (2019). *Race after technology: Abolitionist tools for the New Jim Code*. Polity.
- Butler, J. (2004). *Precarious life: The powers of mourning and violence*. Verso.
- Crenshaw, K. (1991). Mapping the margins: Intersectionality, identity politics, and violence against women of color. *Stanford Law Review*, 43(6), 1241–1299. <https://doi.org/10.2307/1229039>
- D'Ignazio, C., & Klein, L. F. (2020). *Data feminism*. MIT Press. <https://doi.org/10.7551/mitpress/11805.001.0001>
- Galtung, J. (1969). Violence, peace, and peace research. *Journal of Peace Research*, 6(3), 167–191. <https://doi.org/10.1177/002234336900600301>
- GSMA. (2024). *The mobile gender gap report 2024*. GSMA. <https://www.gsma.com/r/gender-gap>
- International Institute for Population Sciences (IIPS), & ICF. (2021). *National Family Health Survey (NFHS-5), 2019–21: India report*. IIPS. <http://rchiips.org/nfhs>
- International Telecommunication Union. (2023). *Measuring digital development: Facts and figures 2023*. ITU. <https://www.itu.int>
- Meta. (n.d.). *Transparency Center: Community standards enforcement [Dataset]*. <https://transparency.meta.com>
- National Crime Records Bureau. (2024). *Crime in India 2023: Statistics*. Ministry of Home Affairs, Government of India. <https://ncrb.gov.in>
- Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. NYU Press. <https://doi.org/10.18574/nyu/9781479833641.001.0001>

- Press Information Bureau. (2023–2025). *Releases on cybercrime trends, 1930 helpline, and I4C initiatives* [Press releases]. Government of India.
<https://pib.gov.in>
- Red Dot Foundation. (n.d.). *Safecity: Crowdsourcing sexual violence reports* [Dataset]. <https://safecity.in>
- The Economist Intelligence Unit. (2021). *Measuring the prevalence of online violence against women*. Economist Intelligence Unit.
<https://onlineviolencewomen.eiu.com>
- UN Women. (2021). *Online and ICT-facilitated violence against women and girls: Policy brief* (citing EIU). <https://www.unwomen.org>
- UNESCO. (2021). *The chilling: Global trends in online violence against women journalists*. UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf0000377223>
- Indian Cyber Crime Coordination Centre. (n.d.). *National Cyber Crime Reporting Portal (1930 helpline): User guidance*. Ministry of Home Affairs.
<https://cybercrime.gov.in>
- MeitY. (2022). *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021—Amendments (2022)*. Ministry of Electronics & Information Technology, Government of India. <https://www.meity.gov.in>
- BBC News. (2022, January 6). *Bulli Bai: India arrests people over app that 'auctioned' Muslim women*. [https://www.bbc.com/news/\[insert-path\]](https://www.bbc.com/news/[insert-path])
- Reuters. (2022, January 4). *'Sulli Deals' app mocked and harassed Muslim women in India; police make arrests*. [https://www.reuters.com/\[insert-path\]](https://www.reuters.com/[insert-path])
- The Times of India. (2024, [Month Day]). *[Exact title about AI-morphed images/sextortion linked to predatory loan apps]*.
[https://timesofindia.indiatimes.com/\[insert-path\]](https://timesofindia.indiatimes.com/[insert-path])
- Internet Freedom Foundation. (2023–2025). *Briefs on harassment via loan apps, doxxing, and impersonation*. Internet Freedom Foundation.
<https://internetfreedom.in>
- United Nations. (2023). *The Sustainable Development Goals report 2023*. UN DESA. <https://unstats.un.org/sdgs/report/2023>