
CYBER HARASSMENT AND ONLINE ABUSE AGAINST NON-BINARY PERSONS: LEGAL CHALLENGES IN INDIA

Ms. Srishti Pandey, School of Legal Studies, Babu Banarasi Das University, Lucknow

Dr. Vatsla Sharma, School of Legal Studies, Babu Banarasi Das University, Lucknow

ABSTRACT

The digital public sphere has turned into a sphere of proportional violence when it comes to non-binary persons in India, that is, individuals whose gender identity surpasses or rejects the binary definitions of man and woman. Cyberstalking, identity-based harassment, nonconsensual disclosure of gender identity (under Indian law), sustained coordinated pile-ons are a unique ecology of online abuse that intersects with the lack of legal recognition of non-binary identities under Indian law. The Information Technology Act, 2000 (with amendments in 2008) the Bharatiya Nyaya Sanhita, 2023, and the Transgender Persons (Protection of Rights) Act, 2019, together form an archipelago of potentially relevant provisions; however, none of them was designed with non-binary persons in mind, and the cumulative coverage that they offer is patchy, uneven, and often unavailable.

This article holds the view that the invisibility of non-binary persons in the legal architecture of India, a creation of the binary gender assumptions embedded in the enumerated grounds of non-discrimination, the Bharatiya Nyaya Sanhita, and the offence structure of the IT Act, turns each instance of cyber harassment into a compounded injury: the original harm of the maltreatment and the secondary harm of legal abandonment. Based on constitutional theory, a comparative legal approach (Canada, the European Union and New Zealand), and a critical reading of the available jurisprudence, the article suggests a series of legislative and judicial reforms aimed at making non-binary persons legally visible and legally protected in the online realm.

I. INTRODUCTION

In May 2022, a non-binary student at a major Indian university was the target of a sustained campaign of anonymous harassment on Instagram and Twitter due to publicly using genderneutral pronouns in one of the campus publications. The messages were either theologically condemnation or even express threats of sexual violence. The officer in charge of the local cyber-crime cell, when approached by the student, is reported to have questioned whether or not the complainant was a man or a woman--a question whose administrative rationale was quite intelligible and whose practical impact was to deprive the complainant of any effective assistance¹. The incident is anecdotal. Its copying throughout the digital ecosystem of India is systemic.

Non-binary persons, individuals who identify beyond the gender binary, including those who identify as genderqueer, genderfluid, agender, bigender, or pangender, are given a queer place in Indian law. This historic ruling by the Supreme Court in *National Legal Services Authority v Union of India* (hereinafter *National Legal Services Authority v Union of India*) acknowledged the constitutional right of transgender individuals to self-identify, and to be recognised by the State in their self-identified gender. This recognition was later given the statutory form by the Transgender Persons (Protection of rights) Act, 2019 (hereinafter 'TPA')². Both the NALSA ruling and the TPA, however, operate within a conceptual framework, which, although formally inclusive, nevertheless perpetuates the privileging of a transition-from-onebinary-to-the-other model of gender identity. Non-binary identities, which do not shift between the poles of the male/female dyad, but instead resist it juridically remain unaddressed.

The outcomes of cyber harassment victims are drastic. The provisions in the Information Technology Act, 2000 (hereinafter 'IT Act') in its amended form were written in a gendered, yet binary manner. The Bharatiya Nyaya Sanhita, 2023 (hereinafter 'BNS') which replaces the Indian Penal Code, 1860, maintains this binary orientation in the provisions on stalking, outraging modesty, and sexual harassment. This leads to a legal system that was originally conceptualized in the binary world, and is currently being applied, with a great deal of difficulty, to experiences which the binary cannot properly capture³. This paper will discuss that challenge in a systematic fashion, posit that the challenge is a constitutional infirmity, and

¹ *National Legal Services Authority v Union of India* (2014) 5 SCC 438 [129]–[135].

² Transgender Persons (Protection of Rights) Act, 2019, Act No. 40 of 2019.

³ Information Technology Act, 2000, Act No. 21 of 2000 (as amended 2008).

suggest the legislative and judicial remedies necessary to overcome it.

This argument is presented in seven sections. Part I charts the terrain of cyber harassment as faced by non-binary individuals in India, based on the available empirical evidence. Part II discusses the coverage, gaps, and interpretive boundaries of the applicable provisions of the IT Act and the BNS. Part III examines the input of TPA into and the constraints of TPA in the cyber-harassment environment⁴. Part IV identifies the legal gaps to a constitutional framework and argues that the failure to include non-binary persons into the effective protection of the law violates Articles 14, 15, and 21 of the Constitution. Part V compares and contrasts Canada, the European Union and New Zealand. Part VI contains a critical study of the interpretive and litigation approaches which can be adopted in the interim. Part VII suggests a set of legislative and judicial reforms⁵.

II. REVIEW OF LITERATURE

Cyber harassment in India has been discussed widely with regards to gendered violence, but the scholarship is still very much limited to the binary concept of gender. Research carried out by the Internet Freedom Foundation and the Centre of Internet and Society have documented trends of online abuse, especially those involving women and LGBTQIA+ individuals, but there is a significant gap in the approaches that address non-binary identities as a separate category of vulnerability⁶.

The implications of information technology act, 2000 and the jurisprudence in the aftermath of the case of *Shreya Singhal v Union of India* has been primarily considered within the context of the implications of the information technology act, 2000 and the jurisprudence that followed in the wake of the case of *Shreya Singhal v Union of India*, specifically in regard to the freedom of speech and intermediary liability⁷. Although these analyses do offer important insights into regulatory constraints, it does not necessarily engage with identity-based harms that go beyond traditional obscenity or harassment paradigms.

It has started to theorize gender identity as a safeguarded attribute in hate speech and

⁴ Bharatiya Nyaya Sanhita, 2023, Act No. 45 of 2023.

⁵ An Act to amend the Canadian Human Rights Act and the Criminal Code, SC 2017, c 3, s 2; Digital Services Act, Regulation (EU) 2022/2065, recital 82.

⁶ Internet Freedom Foundation, *Digital Nagriks: Documenting Online Harassment* (2023) 15–20.

⁷ *Shreya Singhal v Union of India* (2015) 5 SCC 1 [87]–[92].

frameworks of digital harm. These events draw attention to the insufficiency of Indian legal frameworks that still remain in the paradigm of binary⁸.

The article is based on the existing body of knowledge by specifically questioning how nonbinary individuals are legally invisible in the scope of cyber law and constructs a doctrinal and legislative framework, filling this omission.

III. METHODOLOGY

In this research, the research methodology is a doctrinal and comparative research. The doctrinal aspect entails a thorough study of statutory provisions, including the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Transgender Persons (Protection of Rights) Act, 2019, and the relevant judicial precedents, such as *Shreya Singhal v Union of India* and *National Legal Services Authority v Union of India*⁹.

The comparative component of the study analyses legal frameworks in the jurisdictions, including Canada, the European Union, and New Zealand, to determine the best practices in the jurisdiction in addressing issues of identity-based cyber harassment¹⁰. It has used secondary sources such as reports by civil society organisations and academic literature to contextualise the empirical realities of online abuse of non-binary people.

The research is in its core qualitative nature, which aims at identifying gaps in doctrines, limits in interpretation, and deficiency of policies within the current legal framework.

IV. THE LANDSCAPE OF DIGITAL VIOLENCE: NON-BINARY PERSONS IN THE INDIAN CONTEXT

A. Forms and Patterns of Abuse

The cyber harassment experienced by non-binary persons in India is neither random nor merely interpersonal. It is structured by the intersection of three axes of vulnerability: their gender non-conformity, which makes them targets of gender-based online violence; their LGBTQIA+ identity, which exposes them to homophobic and transphobic abuse; and their relative legal

⁸ IT Act, s 66A.

⁹ An Act to amend the Canadian Human Rights Act and the Criminal Code, SC 2017, c 3; Digital Services Act, Regulation (EU) 2022/2065; Harmful Digital Communications Act 2015 (New Zealand).

¹⁰ Internet Freedom Foundation (n 6) 22–28.

invisibility, which means that abusers operate with de facto impunity. Research by the Internet Freedom Foundation, the Centre for Internet and Society, and international organisations including GLAAD and the Association for Progressive Communications has documented several recurring patterns.¹¹

Identity-based harassment encompasses the deployment of misgendering—the deliberate use of pronouns and gendered forms of address that contradict the target's gender identity—as an instrument of humiliation, coordinated across social media platforms. Outing involves the nonconsensual disclosure of a person's non-binary identity to family members, employers, or the public, with consequences that can include employment termination, familial violence, and social ostracism. Non-consensual intimate imagery (NCII), including deepfake sexual content generated through artificial intelligence tools, is deployed specifically against non-binary persons as a mechanism of gendered humiliation and coercive control. Coordinated pile-ons—organised campaigns in which multiple accounts simultaneously direct abuse at a single target, often using platform recommendation algorithms to amplify reach—have been documented against non-binary activists, academics, and public communicators in India.¹²

B. The Empirical Gap

Reliable disaggregated data on cyber harassment against non-binary persons in India is, to state matters plainly, largely absent. The National Crime Records Bureau's annual *Crime in India* reports do not disaggregate cyber-crime victim data by gender identity beyond the binary male/female categorisation. Police cyber-crime cells do not maintain records in a form that would allow identification of non-binary complainants or identity-based targeting. This data gap is itself a form of structural harm: it renders the problem statistically invisible, undermines evidence-based policymaking, and creates a feedback loop in which the absence of data is taken to indicate the absence of a problem.¹³

The available evidence is necessarily derived from community surveys, qualitative research, and civil society documentation. A 2021 survey by the Queerala collective found that 67% of non-binary respondents in Kerala had experienced online harassment specifically referencing their gender identity within the preceding twelve months.¹⁴ Research by the Nazariya Queer

¹¹ *ibid* 30–35.

¹² Nazariya Queer Feminist Resource Group, *Gendered Cyber Harassment and Non-Binary Identities* (2022).

¹³ National Crime Records Bureau, 'Crime in India 2022' (Ministry of Home Affairs) ch 18.

¹⁴ Queerala, 'Online Harassment of Non-Binary Persons in Kerala' (2021) 6–8.

Feminist Resource Group documented that non-binary persons faced disproportionately severe harassment when they used social media to discuss gender identity publicly, with the harassment escalating when the content engaged with religious or caste themes.¹⁵ The Internet Freedom Foundation's *Digital Nagriks* initiative has documented multiple instances of outing campaigns against non-binary individuals, conducted through coordinated action on WhatsApp groups and subsequently amplified on Twitter/X and Facebook.¹⁶

V THE STATUTORY FRAMEWORK

A. The Information Technology Act, 2000

The Information Technology Act, 2000 (hereinafter 'IT Act'), as amended by the Information Technology (Amendment) Act, 2008, contains several provisions potentially applicable to cyber harassment. Section 66A (which criminalised 'grossly offensive' online communications) was struck down by the Supreme Court in *Shreya Singhal v Union of India* as an unconstitutional restriction on freedom of speech under Article 19(1)(a), on the ground of impermissible vagueness. Its removal created a significant gap in the statutory framework for online abuse.¹⁷

Section 66C penalises identity theft and Section 66D penalises cheating by impersonation using computer resources. These provisions are potentially applicable to outing campaigns that involve the creation of fake profiles impersonating a non-binary person, or the use of personal information fraudulently obtained.¹⁸ Section 67 criminalises the publication of obscene material in electronic form, Section 67A criminalises material containing sexually explicit acts, and Section 67B addresses child sexual abuse material. Sections 67 and 67A are relevant to non-consensual intimate imagery (NCII) cases. However, the provisions do not define 'obscene' or 'sexually explicit' with reference to the victim's gender identity, and the existing judicial interpretation of 'obscenity' under the Hicklin test (inherited from *Regina v Hicklin* and applied in *Ranjit D. Udeshi v State of Maharashtra*) does not adequately address the specific harm of gender-identity-based sexual humiliation.¹⁹

¹⁵ Nazariya Queer Feminist Resource Group (n 12) 11–13.

¹⁶ Internet Freedom Foundation (n 5) 30–35.

¹⁷ *Shreya Singhal v Union of India* (2015) 5 SCC 1 [87]–[92].

¹⁸ Information Technology Act 2000, ss 66C, 66D, 67–67B.

¹⁹ *Ranjit D Udeshi v State of Maharashtra* AIR 1965 SC 881.

The most directly relevant provision for sustained harassment is Section 354D of the Indian Penal Code (now Bharatiya Nyaya Sanhita Section 78), which criminalises stalking, including digital stalking — ‘monitoring the use by a woman of the internet, email or any other form of electronic communication.’ The provision is explicitly gendered: it protects only ‘a woman.’ A non-binary person who identifies neither as man nor as woman has no standing under this provision. The same structural exclusion applies to Section 354A (sexual harassment) and Section 354B (assault or criminal force with intent to disrobe), preserved as Sections 74, 75, and 76 of the Bharatiya Nyaya Sanhita, all of which are framed around protection of ‘a woman.’²⁰

B. The Bharatiya Nyaya Sanhita, 2023: Continuity Of Binary Assumptions

The Bharatiya Nyaya Sanhita, 2023 (hereinafter ‘BNS’) was presented, in the political discourse surrounding its enactment, as a comprehensive modernisation of Indian criminal law. For non-binary persons, however, the BNS represents a missed legislative opportunity of considerable magnitude. The parliamentary debates preceding its enactment contain no sustained engagement with gender identity as a dimension of criminal vulnerability, and the enacted text preserves the binary framework of the Indian Penal Code with minimal modification.²¹

Section 351 of the BNS (criminal intimidation) and Section 352 (intentional insult) are gender-neutral in their structure and are therefore technically available to non-binary complainants. However, these provisions do not specifically address the identity-based dimension of cyber harassment: they provide no enhanced penalty for harassment motivated by gender identity, and their evidentiary requirements are ill-suited to the diffuse, multi-platform, often anonymous character of coordinated online abuse.²² Section 356 of the BNS (defamation) is similarly gender-neutral but again lacks specific application to identity-targeted harassment.²³

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (hereinafter ‘IT Rules, 2021’), issued under Sections 79 and 87 of the IT Act, impose obligations on significant social media intermediaries to establish grievance redressal mechanisms and to act against content violating specified categories, including ‘content that is

²⁰ Bharatiya Nyaya Sanhita 2023, ss 74–78; Indian Penal Code 1860, s 354D.

²¹ Bharatiya Nyaya Sanhita 2023, Statement of Objects and Reasons.

²² Bharatiya Nyaya Sanhita 2023, ss 351–352.

²³ Bharatiya Nyaya Sanhita 2023, s 356.

grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy.'²⁴ While gender-identity-based harassment may theoretically fall within 'harassing' content, the Rules do not identify gender identity as a protected characteristic, and intermediaries are not required to maintain data on the gender identity of complainants or the identity-based character of reported abuse.²⁵

C. The IT (Amendment) Bill, 2023 And The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (hereinafter 'DPDPA') introduces a framework for consent-based processing of personal data, including 'sensitive personal data,' which encompasses data 'related to sexual orientation.' Non-binary gender identity falls within this category, at least by necessary implication. The DPDPA's requirements of consent for data collection, right to erasure, and right to grievance redressal are potentially significant tools for non-binary persons targeted by outing — the non-consensual disclosure of gender identity constitutes processing of sensitive personal data without consent.²⁶

However, the DPDPA's enforcement mechanism (through the Data Protection Board) is untested, its remedies are primarily compensatory rather than preventive, and its provisions do not specifically address the weaponisation of identity data in online harassment campaigns.²⁷

VI. THE TRANSGENDER PERSONS ACT, 2019

The Transgender Persons (Protection of Rights) Act, 2019 (hereinafter 'TPA') provides a statutory framework that, on its face, might appear to extend protection to non-binary persons. Section 3 prohibits discrimination against transgender persons in a range of contexts, including employment, education, and access to services. Section 18 criminalises 'abuse, violence, and exploitation' of transgender persons, with a maximum sentence of two years' imprisonment. On a generous reading, Section 18 encompasses cyber harassment of transgender persons — 'abuse' is not defined and could include online abuse — and the provision is not confined to physical violence.²⁸

The difficulties are, however, substantial. First, the TPA's definition of 'transgender person'

²⁴ *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021*, rr 3(1)(b), 3(2).

²⁵ Ministry of Electronics and Information Technology, 'IT Rules Compliance Framework' (2021).

²⁶ Digital Personal Data Protection Act 2023, ss 2, 4, 8.

²⁷ *ibid* s 33 (Data Protection Board).

²⁸ Transgender Persons (Protection of Rights) Act 2019, ss 3, 18.

under Section 2(k) — ‘a person whose gender does not match with the gender assigned at birth’ — is broad enough to include some non-binary persons, but the Act’s conceptual architecture assumes a movement from one binary gender to another or a liminal position between the two binary poles. Persons who identify as agender (without gender) or as entirely outside the male/female spectrum may not squarely fall within this definition, and there is no judicial guidance on the question.²⁹

Second, even where the TPA’s protections technically apply, the enforcement mechanism is chronically deficient. The National Council for Transgender Persons established under Section 16 of the TPA is primarily an advisory body; it has no investigative or prosecutorial authority. State-level complaint mechanisms are inconsistently established and, where they exist, officers frequently lack training in gender-identity issues. A non-binary complainant reporting cyber harassment under Section 18 of the TPA faces the simultaneous challenges of establishing their identity as a ‘transgender person’ within the Act’s definition, identifying a competent investigating authority, and persuading investigators that online abuse constitutes ‘abuse’ for purposes of the provision.³⁰

Third, and most fundamentally, the TPA contains no provision analogous to the Protection of Women from Domestic Violence Act’s (PWDVA) civil remedial framework: no protection order mechanism, no emergency relief, no equivalent of the Protection Officer. The criminal sanction in Section 18 requires a full criminal prosecution — a process that, in the Indian context, typically takes years, exposes the complainant to cross-examination on their gender identity, and results in conviction in a fraction of cases. For victims of sustained online abuse who require urgent relief — removal of content, cessation of harassment, restriction on the abuser’s online access — the TPA offers nothing.³¹

VII. CONSTITUTIONAL DIMENSIONS: THE RIGHT TO DIGNITY IN DIGITAL SPACE

A. Article 14 And The Equal Protection Deficit

The equal protection guarantee of Article 14 of the Constitution of India requires that ‘all persons are equally entitled to equal protection of laws.’ The legal framework for cyber

²⁹ *ibid* s 2(k).

³⁰ Ministry of Social Justice and Empowerment, ‘Implementation Status of TPA’ (2022).

³¹ Protection of Women from Domestic Violence Act 2005.

harassment, as described above, protects ‘women’ (under the BNS stalking and sexual harassment provisions) and, to a limited extent, ‘transgender persons’ (under the TPA). Non-binary persons who are not ‘women’ and do not fall clearly within the TPA’s definition of ‘transgender person’ are denied equivalent protection. Under the standard classification test articulated in *State of West Bengal v Anwar Ali Sarkar*, this differential treatment requires justification through a reasonable classification with a rational nexus to a legitimate legislative object.³²

No such nexus is apparent. The object of the BNS’s anti-stalking and sexual harassment provisions is the protection of vulnerable individuals from identity-based online abuse.

Non-binary persons are at least as vulnerable to such abuse as women, and in many documented cases are more vulnerable, given the compound effect of gender non-conformity stigma and legal invisibility. The exclusion of non-binary persons from the protective ambit of these provisions does not serve the stated legislative object; it frustrates it. The substantive equality framework developed in *Anuj Garg v Hotel Association of India* requires the court to examine whether the classification perpetuates existing disadvantage, and the exclusion of non-binary persons from legal protection against cyber harassment paradigmatically does so.³³

B. Article 15 And Discrimination On The Ground Of Sex

The Supreme Court’s unanimous holding in *Navtej Singh Johar v Union of India* that ‘sex’ in Article 15(1) encompasses sexual orientation and gender identity provides the constitutional foundation for a discrimination-based challenge to the binary architecture of Indian cyber-harassment law. If the State discriminates on the ground of gender identity by failing to extend legal protection against cyber harassment to non-binary persons, while extending equivalent protection to persons of binary genders, such discrimination violates Article 15(1). Justice D.Y. Chandrachud’s concurring opinion in *Navtej* specifically acknowledged that ‘the denial of the right to sexual orientation is a denial of the right to dignity’ — a formulation directly applicable to the denial of legal protection against identity-based digital abuse.³⁴

The *K.S. Puttaswamy v Union of India* (Privacy) judgment’s recognition of informational privacy as a dimension of constitutional dignity is particularly significant in the cyber-harassment context. Justice Chandrachud’s opinion identified the right to control the narrative

³² *State of West Bengal v Anwar Ali Sarkar* AIR 1952 SC 75.

³³ *Anuj Garg v Hotel Association of India* (2008) 3 SCC 1.

³⁴ *Navtej Singh Johar v Union of India* (2018) 16 SCC 368 [377]–[381].

of one's own identity as a core component of the right to privacy: 'the ability of the individual to prevent others from imposing a narrative upon them.' The outing of non-binary persons — the non-consensual disclosure of their gender identity — is a direct violation of this right. The State's failure to provide an effective legal remedy against outing, through the IT Act or any other instrument, constitutes a failure of the positive obligation to protect constitutional rights that the *Puttaswamy* judgment implies.³⁵

C. Article 19(1)(A) And The Chilling Effect On Digital Expression

The Supreme Court in *Maneka Gandhi v Union of India* established that the rights guaranteed under Part III of the Constitution are not independent silos but form an integrated framework. The freedom of speech and expression guaranteed under Article 19(1)(a) must be read in conjunction with the Article 21 right to dignity and the Article 14 right to equal protection. For non-binary persons, the absence of legal protection against cyber harassment produces a 'chilling effect' on digital expression: the rational calculation that public expression of one's gender identity will attract coordinated abuse for which no adequate legal remedy exists will deter such expression entirely. This chilling effect is itself an Article 19(1)(a) harm — it restricts the freedom of expression of a group defined by the constitutionally protected characteristic of gender identity.³⁶

The chilling effect argument has been judicially recognised in the context of online expression more broadly. In *Shreya Singhal v Union of India*, the Supreme Court struck down Section 66A of the IT Act precisely because its vagueness produced a chilling effect on constitutionally protected speech. By analogy, a legal framework that fails to protect non-binary persons from online abuse produces a chilling effect on the constitutionally protected expression of gender identity — an outcome equally incompatible with the free-speech guarantee.³⁷

VIII. COMPARATIVE INSIGHTS

A. Canada: The Non-Binary Benchmark

Canada's *An Act to amend the Canadian Human Rights Act and the Criminal Code* (Bill C-16, 2017) amended the *Canadian Human Rights Act* to add 'gender identity or expression' as a prohibited ground of discrimination and amended Section 319 of the *Criminal Code* to add the

³⁵ *KS Puttaswamy v Union of India* (2017) 10 SCC 1 [298].

³⁶ *Maneka Gandhi v Union of India* AIR 1978 SC 597.

³⁷ *Shreya Singhal v Union of India* (2015) 5 SCC 1 [87].

same ground to the list of identifiable groups protected against hate propaganda. The Criminal Code amendment is directly relevant: it criminalises the public incitement of hatred and the wilful promotion of hatred against groups defined by gender identity or expression, without requiring that the victim be of binary gender.³⁸

Canadian human rights tribunals have consistently recognised non-binary persons as protected under ‘gender identity or expression.’ The British Columbia Human Rights Tribunal’s decision in *Comber v School District No. 57* held that the deliberate and sustained misgendering of a non-binary employee constituted discrimination on the ground of gender identity. The tribunal’s reasoning — that misgendering is not merely offensive but constitutive of discrimination, in that it denies the target’s identity — provides a doctrinal template for the recognition of identity-targeted cyber harassment as a form of discrimination rather than merely a personal insult.³⁹

B. The European Union: Platform Accountability And Identity-Based Hate

The European Union’s *Digital Services Act* (DSA, Regulation (EU) 2022/2065), which entered full application in February 2024, imposes obligations on Very Large Online Platforms (VLOPs) to assess and mitigate systemic risks arising from the design and functioning of their services, including risks to ‘fundamental rights.’ Recital 82 of the DSA specifically identifies ‘gender-based violence’ as a systemic risk that VLOPs must address. While the DSA does not define ‘gender’ in binary terms, the European Commission’s guidance documents have indicated that ‘gender-based violence’ includes violence based on gender identity, encompassing non-binary identities.⁴⁰

The DSA model is instructive for India because it places responsibility on platforms — not merely on individual perpetrators — for the systemic dimensions of online abuse. The IT Rules, 2021 move in this direction but do not go nearly as far: they impose grievance-redressal obligations on intermediaries but do not require systemic risk assessment, do not identify gender identity as a protected characteristic, and do not mandate transparency reporting on the identity-based character of removed content.⁴¹

³⁸ *An Act to amend the Canadian Human Rights Act and the Criminal Code*, SC 2017, c 3.

³⁹ *Comber v School District No 57* 2019 BCHRT 175.

⁴⁰ *Digital Services Act, Regulation (EU) 2022/2065*, recital 82.

⁴¹ Harmful Digital Communications Act 2015 (NZ), s 3.

C. New Zealand: Recognition Without Limitation

New Zealand's *Harmful Digital Communications Act 2015* (HDCA) is perhaps the most directly relevant comparative model. The HDCA creates a specific cause of action for harmful digital communications, defined as communications that 'cause harm' to the target — a definition broad enough to encompass all forms of cyber harassment irrespective of the target's gender identity.⁴² The HDCA established a specialist Approved Agency (NetSafe) to receive complaints and facilitate resolution, with judicial recourse available through the District Court.

Critically, the HDCA's harm-based framework does not require the complainant to fit within a binary gender category: the statutory protection extends to 'an individual,' without qualification.⁴³

New Zealand's *Human Rights Act 1993* and the *Human Rights (Gender Identity and Intersex Status) Amendment Act 2023* further extend anti-discrimination protection to persons of all gender identities, including non-binary, in a manner that can be invoked in civil proceedings against both individual harassers and institutional actors. The New Zealand model demonstrates that a harm-based, identity-neutral statutory framework is both legislatively achievable and practically functional.⁴⁴

IX. CRITICAL ANALYSIS: CURRENT STRATEGIES AND THEIR LIMITS

A. Platform Grievance Mechanisms

In the absence of effective state legal remedies, non-binary victims of cyber harassment in India frequently rely on the internal content moderation and grievance-redressal systems of social media platforms. Major platforms — Meta (Facebook, Instagram), Twitter/X, and Google/YouTube — maintain Community Standards or Terms of Service that nominally prohibit harassment based on gender identity. The practical effectiveness of these mechanisms is, however, severely constrained by the scale at which platforms operate, the inconsistency of moderation decisions across language and context, and the absence of any legal obligation to

⁴² *Human Rights Act 1993 (NZ)*; *Human Rights (Gender Identity and Intersex Status) Amendment Act 2023*.

⁴³ Ministry of Justice (New Zealand), 'Harmful Digital Communications Act Review' (2020).

⁴⁴ *Human Rights Act 1993 (NZ)* as amended by the *Human Rights (Gender Identity and Intersex Status) Amendment Act 2023*; discussion of expanded ground-of-discrimination coverage.

report or act on identity-based harassment in the Indian regulatory framework.⁴⁵

The IT Rules, 2021 require significant social media intermediaries to appoint a Grievance Officer, to acknowledge complaints within twenty-four hours, and to dispose of complaints within fifteen days. However, the Rules do not require platforms to maintain or disclose data on the identity-based character of harassment complaints, and the Grievance Officer's decisions are not subject to any external audit or quality assurance process. The Supreme Court's observation in *Shreya Singhal* that intermediary liability frameworks must be interpreted consistently with fundamental rights has not been operationalised in a form that specifically protects non-binary persons.⁴⁶

B. PIL Litigation: Promise And Peril

Several public interest litigations have sought judicial intervention on the inadequacy of cyber harassment law for LGBTQIA+ persons, including non-binary individuals. The Delhi High Court, in a series of orders in matters arising from the NALSA judgment's implementation, has directed the Central Government to provide training to police personnel on LGBTQIA+ issues and to establish designated complaint mechanisms.⁴⁷ These orders have produced limited practical implementation. The more fundamental difficulty with PIL as a strategy for non-binary cyber harassment is that the constitutional challenge required — a facial challenge to the binary architecture of the BNS and IT Act — demands a degree of doctrinal development that the Supreme Court, given its restraint in *Supriyo v Union of India*, may not be immediately prepared to undertake.⁴⁸

The more promising immediate litigation strategy may be a directed challenge under Article 226 to specific executive inactions: the failure of the National Crime Records Bureau to collect disaggregated data on cybercrime victims by gender identity; the failure of the Ministry of Electronics and Information Technology to issue guidelines recognising gender identity as a protected characteristic under the IT Rules, 2021; and the failure of state governments to train cyber-crime cell officers in the handling of identity-based harassment complaints. These challenges seek to compel compliance with existing constitutional obligations rather than to

⁴⁵ Internet Freedom Foundation (n 5) 30–35.

⁴⁶ *Shreya Singhal v Union of India* (2015) 5 SCC 1.

⁴⁷ NALSA (n 1).

⁴⁸ *Supriyo v Union of India* (2023) SCC OnLine SC.

create new law and are correspondingly less vulnerable to the restraint objection.⁴⁹

X. REFORM-ORIENTED CONCLUSION: TOWARDS LEGAL VISIBILITY

The foregoing analysis establishes a clear proposition: non-binary persons in India are exposed to distinctive and disproportionate patterns of cyber harassment, and the legal framework available to them is constitutionally deficient, structurally binary, and practically inaccessible. The deficiency is simultaneously legal (in the inadequacy of statutory provisions), administrative (in the absence of trained personnel and data collection systems), and political (in the persistent unwillingness of the legislative branch to address gender identity beyond a binary-transition model). Curing the deficiency requires action at each of these levels.⁵⁰

The first and most fundamental reform is the amendment of Section 2(k) of the *Transgender Persons (Protection of Rights) Act, 2019* to explicitly include non-binary, genderqueer, agender, bigender, and intersex individuals within the class of protected persons, and to enumerate these identities by reference to international human rights standards — specifically the *Yogyakarta Principles Plus 10* (2017), which represent the authoritative international articulation of the application of human rights law to sexual orientation, gender identity, and gender expression.⁵¹

The second reform is the enactment of a dedicated *Harmful Digital Communications Act* modelled on the New Zealand HDCA, establishing a harm-based, identity-neutral framework for cyber harassment that extends to all persons irrespective of gender identity. Such legislation should establish an independent Digital Communications Ombudsman with the power to order content removal, issue cease-and-desist directions, require intermediaries to disable abusive accounts, and award compensation. The ombudsman's jurisdiction should encompass complaints from persons of all gender identities, with enhanced remedies for identity-targeted harassment.⁵²

The third reform is the amendment of the BNS stalking and sexual harassment provisions (Sections 74, 75, 76, and 78) to replace 'a woman' with 'any person,' following the model of the United Kingdom's *Protection from Harassment Act 1997*. This amendment should be

⁴⁹ Constitution of India, art 226.

⁵⁰ Internet Freedom Foundation (n 5) 30–35.

⁵¹ *Yogyakarta Principles Plus 10* (2017).

⁵² Harmful Digital Communications Act 2015 (NZ).

accompanied by the introduction of an aggravated offence of ‘identity-based harassment’ — harassment motivated by the victim’s actual or perceived gender identity or sexual orientation — carrying an enhanced penalty, on the model of the hate-crime aggravation provisions in the *Canadian Criminal Code* and the *UK Crime and Disorder Act 1998*.⁵³

The fourth reform is regulatory: the Ministry of Electronics and Information Technology should amend the *IT Rules, 2021* to expressly identify gender identity as a protected characteristic and to require significant social media intermediaries to: (a) maintain and publish disaggregated data on harassment complaints categorised by the protected characteristic targeted; (b) implement specific product-design measures to reduce algorithmic amplification of identity-based harassment; and (c) provide a dedicated reporting mechanism for identity-targeted abuse, including a mandatory review timeline shorter than the general fifteen-day period.⁵⁴

The fifth reform is institutional: the National Crime Records Bureau should be directed, by the Ministry of Home Affairs, to revise its cybercrime-data collection framework to capture gender identity as a victim characteristic distinct from binary gender. Simultaneously, the National Police Academy and state police-training institutions should incorporate training on gender identity, non-binary identities, and identity-based cyber harassment into their curricula for cyber-crime investigators.⁵⁵

The sixth reform is constitutional: the Supreme Court should be invited, in an appropriate case, to hold that Articles 14, 15, and 21 of the Constitution — read in light of *Navtej Singh Johar*, *K.S. Puttaswamy*, and *NALSA* — impose a positive obligation on the State to provide effective legal protection against identity-based cyber harassment to non-binary persons, and that the current statutory framework’s failure to do so constitutes an unconstitutional omission. Such a holding would create the constitutional imperative for legislative action that has thus far been absent.⁵⁶

The deeper issue, of which all the above are symptoms, is one of legal imagination. The law’s capacity to protect depends on its capacity to see. A legal system that sees only men and women

⁵³ Protection from Harassment Act 1997 (UK); Crime and Disorder Act 1998 (UK).

⁵⁴ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, rr 3(1)(b), 3(2).

⁵⁵ National Crime Records Bureau, ‘Crime in India 2022’ (Ministry of Home Affairs).

⁵⁶ *Navtej Singh Johar v Union of India* (2018) 16 SCC 368; *KS Puttaswamy v Union of India* (2017) 10 SCC 1.

⁵⁷ *Yogyakarta Principles Plus 10* (2017).

cannot see the harms directed at those who are neither — nor who are more than both. Non-binary persons are not an anomaly or an edge case. They are persons, entitled as a matter of constitutional right to the full protection of the legal order. The digital public sphere, in which an increasing proportion of social life is conducted, must become as safe for them as for anyone else. It will not become so without legal intervention that is as imaginative as the identities it is designed to protect.⁵⁷