“Anti-C~~(Y)~~ber Bullying Policy”

A Policy Proposal to Tackle Cyberbullying in Educational Institutions in India

Authors:

Anwin Thomas K, [a] Sagnik Sarkar, [a] Shambhavi Sharma [a]

[a] Students of Year III, B.A. LL.B. (Hons.), Tamil Nadu National Law University

Presented at:

The NLIU Policy Case Competition 2021

April 2021

Executive Summary

The fast paced digital spaces have become an extension of our physical existence and so have the institutions which were earlier limited to the offline world. This has also given rise to the problems surrounding delinquent activities such as cyber bullying. Online harassment is often done with the intention to humiliate the victim and subject them to social harms, irrespective of its implications, cyberbullying continues to be a commonplace among student populations in universities. The lack of a robust legal framework, redressal and institutional support worsen the problem, it is therefore important for educational institutions to *observe, act. and inspire*, safer online behaviour and spaces.

A number of jurisdictions globally have attempted to define cyberbullying in various legal instruments. All of these definitions, unfortunately, are overbroad and therefore infringe on free speech. The Indian legal framework presently has no definition of cyberbullying, and it is difficult to fit every instance into the pigeon-hole of an existing civil, or criminal, wrong. We propose an objective definition of cyberbullying. This definition must be discovered by a sample survey of persons with internet access, mental healthcare professionals, and legal experts, to arrive at an objective definition that protects persons from cyberbullying to the fullest extent possible while not infringing on free speech.

The institutional enforcement mechanism suggested is a comprehensive one with focus on ways to reduce cyber-bullying. Tackling cyber-bullying by holding offenders accountable at the same time respecting due process rights of the same alleged offender and channelling appropriate resources for the victim to reduce the harm brought in by cyberbullying. We focus on a fair impartial process. Even while the whole world loses respect for due process, we believe that it is non-negotiable.

Table of Contents

1. Introduction

India's continually expansive internet penetration [1] and the digital footprint [2] of its citizens has helped bridge many gaps in terms of access to internet resources, however, the flip side of the coin is that electronic communication media has also exposed the users to the risks of online harassment [3] and other innumerable consequences which are often not sufficiently encompassed in a single term 'cyber bullying'. [4]

1.1. The Social Dimensions of Cyberbullying

Internet communication comes with inherent anonymity [5] coupled with informational dynamism which can potentially put an individual's personal security, privacy, data etc at risk. [6] These variables are secondary in securing online space when studied in contrast to the social risks of online aggressions which have far overreaching consequences in the form of social costs of performance and sociality for student victims. [7] Studies reflect varying results due to different areas of focus and lack of a common definition of cyberbullying, [8] However, largely, US based literature indicates that, 34% of college students have experienced cyberbullying as victims; 64% of students have observed cyberbullying of other student victims, and 19% have been perpetrators of cyberbullying victimization. Further literature

---

[1] Internet and Mobile Association of India (IMAI), "Digital in India 2019: Round 2 Report" (Nielsen, 2019).

[2] McKinsey Global Institute, "Digital India: Technology to transform a connected nation", *available at* https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20india%20technology%20to%20transform%20a%20connected%20nation/digital-india-technology-to-transform-a-connected-nation-full-report.ashx (last visited on April 09, 2021).

[3] Anuradha Shetty, "India Ranks Third on Global Cyber Bullying List-Technology News", *Firstpost*, June 28, 2012, *available at* https://www.firstpost.com/tech/news-analysis/india-ranks-third-on-global-cyber-bullying-list-3602419.html (last visited on April 09, 2021).

[4] Gökhan Atik, "Assessment of school bullying in Turkey: A critical review of self-report instruments" 15 *Procedia Social and Behavioral Sciences* 3232 (2019); Michael J. Furlong, Jill D. Sharkey, Erika D. Felix, Diane Tanigawa, Jennifer Greif Green, "Bullying assessment: A call for increased precision of self-reporting procedures" in S. R. Jimerson, S. M. Swearer, & D. L. Espelage (eds.), *Handbook of bullying in schools: An international perspective* 329-345 (Routledge, 2010).

[5] S. Phillips, "Coping with cyberbullying: The use of technology to terrify", *Public Broadcasting Service (PBS), This Emotional Life*, October 19, 2010.

[6] Child Rights and You (CRY), *Online Safety and Internet Addiction (A Study Conducted Amongst Adolescents in Delhi-NCR)* (2020).

[7] J.S. Wong, "The cruel reality of student cyberbullying", *College Degrees*, January 19, 2011.

[8] Sameer Hinduja and Justin W. Patchin, *Cyberbullying Fact Sheet* 5 (Cyberbullying Research Center, 2010), *available at* https://cyberbullying.org/cyberbullying-fact-sheet-identification-prevention-and-response (last visited on April 09, 2021).

indicates increased homophobic incidents and sexting of student victims, 39% as female victims and 25% as male victims. [9]

This situation has significantly reached an alarming threshold which has resulted in the *normalisation* of cyberbullying. Further, an increasing-one sided focus on victim restoration centric approach with the absence of any structural respite which indicates a settling 'diffusion of responsibility' among stakeholders. [10] Scholars have also pointed out that when such offences become commonplace phenomena, individuals no longer feel responsible to respond to such emergencies, also known as the bystander effect. [11] This structural normalization of bullying in digital spaces has also affected the *agency of the victims* to approach the relevant authorities when met with harassment, largely because, more often the victims themselves don't identify the action being done to them as bullying. [12] Another obvious cause for the under reporting of cases is lack of access and knowledge of legal remedies available.

1.2. The Inadequacy of the Present Indian Cyber Law Regime

The American Academy of Pediatrics defines cyber bullying as, "deliberately using digital media to communicate false, embarrassing, or hostile information about another person." [13] The National Crime Prevention Council (US) defines it as, "the process of using the Internet, cell phones or other devices to send or post text or images intended to hurt or embarrass another person." [14] This definition is a sufficient reflection of the general contours of cyberbullying.

---

[9] Robert S. Tokunaga, "Following you home from school: A critical review and synthesis of research on cyberbullying victimization" 26(3) *Computers in Human Behavior* 277 (2010); Susan M. Swearer, "Five myths about bullying", *The Washington Post*, December 30, 2010, *available at* https://www.washingtonpost.com/wp-dyn/content/article/2010/12/30/AR2010123001751.html (last visited on April 09, 2021).

[10] Nishant Shah, "Staying silent about cyberbullying is no longer an option", *The Indian Express*, June 16, 2019, *available at* https://indianexpress.com/article/express-sunday-eye/cyberbullying-is-the-dangerous-new-normal-5780934/ (last visited on April 09, 2021).

[11] Mary Aiken, *The Cyber Effect: A Pioneering Cyberpsychologist Explains How Human Behaviour Changes Online* 119-138 (Hachette, UK, 2016).

[12] *Supra* note 10.

[13] Gwenn Schurgin O'Keeffe and Kathleen Clarke-Pearson, "Clinical Report— The Impact of Social Media on Children, Adolescents, and Families", American Academy of Pediatrics, *available at* http://doi.org/10.1542/peds.2011-0054 (last visited on April 06, 2021).

[14] John Chapin, "Adolescents and Cyberbullying: The Precaution Adoption Process Model" 21(4) *Education and Information Technologies* 719 (2016).

In a legal sense, cyberbullying is materially different from other tortious, and criminal, wrongs. It is difficult to fit cyberbullying into the pigeon-hole of an existing tort. [15] The most common candidate is the tort of defamation. However, defamation requires the lowering of the reputation of the victim in the eyes of society,[16]which is not a necessary ingredient of every instance of cyberbullying. It is very much possible for cyberbullying to take place without causing a lowering of the reputation of the victim in the eyes of society. [17] Similarly, it is difficult to fit all cyberbullying into existing criminal wrongs. [18] Stalking, and various forms of harassment (sexual or otherwise), are the candidates. The definitions of stalking, and various forms of harassment, in criminal law statutes tend to be narrower than the fullest possible ambit of cyberbullying. [19]

Keeping aside the limitations of the definitions in the Indian statutes which have not yet defined 'cyber bullying' *per se*, a conjunctive reading of the provisions of the Information Technology Act, 2000 ("IT Act") and the Indian Penal Code, 1860 ("IPC") can help the victims get remedy in a few instances, such as, cyber stalking and online sexual harassment. For example, the definition of stalking under Section 354D of IPC, which penalises "any man who monitors the use by a woman of the internet, email or any other form of electronic communication," [20] falls short on two accounts: *first*, the section is not gender neutral, meaning that a male victim of stalking online cannot seek remedy; and *second*, there is no clarity as to what actions constitute as 'monitoring' and 'watching'. [21]

Cases of online sexual harassment, such as an instance of creating a fake profile and maligning the image of an individual online, may constitute an offence under Sections 354A (sexual harassment and punishment for sexual harassment), S. 354D (stalking), and S. 499, read with S. 500 (defamation), S. 507 (criminal intimidation by anonymous communication), and S. 509 (word, gesture or act intended to insult the modesty of a woman), of IPC.[22] The obvious limitation of all these provisions is the anonymity of the internet itself, which may

---

[15] "Cyberbullying: Holding Grownups Liable for Negligent Entrustment" 49(2) *Houston Law Review* 532 (2012), p. no. 543-545.
[16] Edwin Peel and James Goud Kamp, *Winfield and Jolowicz on Tort* 1039 (Sweet and Maxwell, 19th edn., 2014).
[17] *Id.* at 10-11.
[18] Alison M. Smith, *Protection of Children Online: Federal and State Laws Addressing Cyberstalking, Cyber Harassment, and Cyberbullying* 4-11 (US Congressional Research Service, Washington, D.C., 2009).
[19] *Id.*
[20] The Indian Penal Code, 1860 (Act 45 of 1860), ss. 354A, 345D.
[21] *State of West Bengal v. Animesh Boxi*, GR No. 1587 of 2017.
[22] *Sazzadur Rahman v. The State of Assam*, Crl. No. 654 of 2019; *Shubham Bansal v. State (Govt. of NCT Delhi),* Crl. Misc. No. 2024 of 2018; *Jitender Singh Grewal v.State of West Bengal,* Crl. Misc. No. 7252 of 2018.

render these provisions ineffective in the absence of a robust structure to tackle the peculiarities of cyber stalking as a separate offense. Thus, while some cyberbullying can most definitely be into the definitions of these existing criminal wrongs, other less serious forms of cyberbullying will escape from their ambit. Especially in India, where there appears to be no definition of cyberbullying in any past, or present, legal instrument.

1.3. Institutional Cyberbullying Policies: Need of the Hour

The shortcomings of the legal framework coupled with the lack of awareness of the social consequences of cyberbullying in institutional spaces, leads to the problem of unreported cases among victims.[23] It is thus incumbent upon the institutional authorities to cater to the needs of the student population [24] by creating safe spaces in the form of institutional bodies which help them get access to both legal and psychological remedies.[25]

2. Scope and Applicability

This policy proposal has been drafted with the objective of ensuring a safe and healthy environment in universities, keeping in mind the increasingly digital dimensions of higher education institutions.

The jurisdictional scope of the proposed policy will extend to:

1. The physical premises of the campus of the University, and:
    a. All digital spaces which can be termed as a notional extension of the University's premises;
    b. Any other online space where the subjects of this policy may interact among each other or/and with a third person.
2. The above jurisdictional scope shall extend to all the following persons, regardless of them being the victim or the perpetrator of the cyberbullying in question:
    a. *All* students enrolled in the university in the current academic year.
    b. *All* the employees, academic staff and faculties of the university. 'Employees' means any person appointed by the University on permanent basis or

[23] N. Gomez, "Cyberbullying: The nation's epidemic", *Converge*, December 14, 2010.
[24] Paul F. Brain and Peter K. Smith, "Bullying in schools: Lessons from two decades of research" 26(1) *Aggressive Behavior* 1 (2000).
[25] *Id.*

temporary basis, full-time or part-time or under contract, and who has recognized rights and duties.

c. *Any other person* who may be connected to the university in the capacity of an event participant or a visitor.

3. Defining Cyberbullying

For any policy framework to effectively tackle cyberbullying, it is necessary to define cyberbullying itself at the very outset.

The need to protect persons against cyberbullying engages with the countervailing interest of securing the right to freedom of speech and expression. It is possible to define cyberbullying in a manner which encompasses constitutionally protected speech. Thus, in the search for a definition of cyberbullying, there are two competing interests at stake: the protection of persons from the injuries of being subject to cyberbullying, vis-a-vis ensuring the right to freedom of speech and expression. Both of these are legitimate interests the State is obliged to secure. [26] Hence, the definition of cyberbullying must fairly balance these conflicting interests. [27] An overinclusive definition will have a 'chilling effect' on free speech, whereas an underinclusive definition will fail to sufficiently protect persons against cyberbullying.

3.1. The Inadequacy of Existing Legal Definitions of Cyberbullying

Some foreign jurisdictions have attempted to define cyberbullying in various enacted, or proposed, legal instruments. A Bill introduced in US Congress in 2009 proposed to define cyberbullying as, "any communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person, using electronic means to support severe, repeated, and hostile behavior…" [28] US Federal Law contains a useful definition of harassment, although not cyberharassment. In that context, harassment has been defined as, "a serious act or course of conduct directed at a specific person that... causes substantial emotional distress

---

[26] The Constitution of India, art. 13(2); Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy" 4(5) *Harvard Law Review* 193 (1890), p. no. 193-197.

[27] Chester James Antieau, "The Jurisprudence of Interests as a Method of Constitutional Adjudication" 27 *Case Western Law Review* 823 (1977), p. no. 833, 843-857; T. Alexander Aleinikoff, "Constitutional Law in the Age of Balancing" 96(5) *Yale Law Journal* 943 (1987), p. no. 945-948; Kai Moller, "Proportionality: Challenging the critics" 10(3) *International Journal of Constitutional Law* 709 (2012), p. no. 711-716; Kai Moller, "U.S. Constitutional Law, Proportionality, and the Global Model" in Vicki Jackson and Mark Tushnet (eds.), *Proportionality: New Frontiers, New Challenges* (Cambridge, 2016); *Modern Dental College and Research Centre v. State of Madhya Pradesh* (2016) 7 SCC 353.

[28] *Supra* note 18 at 10.

in such person; and serves no legitimate purpose…" [29] A number of US states have enacted laws to regulate cyberstalking and cyberharassment, but not cyberbullying specifically, which is a materially different wrong. [30] Few US states have enacted laws which specifically define cyberbullying. For instance, a Missouri State Law defines cyberbullying as, "knowingly [frightening], [intimidating], or [causing emotional distress] to another person by anonymously making a telephone call or any electronic communication". [31] A New Zealand law defines cyberbullying as consisting of, disclosure of "sensitive personal facts", a communication that is "threatening, intimidating or menacing", an "indecent or obscene" communication, the making of a "false allegation", etc. [32] While the New Zealand law seems to be marginally more precise than its US counterparts, the definitions of cyberbullying in all of these laws appear to be quite generally, and broadly, worded. None of them precisely identify which particular conducts would constitute cyberharassment.

It is necessary to state the definition of cyberbullying with a fair degree of precision. If the definition is couched quite broadly and generally, such as the definitions found in public health literature or in the US statutory instruments discussed above, there is a risk it can be found unconstitutional due to overbreadth. The right to equality before law, guaranteed by the Constitution, protects every person against arbitrary conduct. [33] When a statutory provision is drafted in broad, and fairly imprecise, language, it can be interpreted in multiple ways at the pleasure of the enforcing authorities to prohibit, or not prohibit, a wide variety of uncertain conducts. [34] Overbroad decisions thus enable authorities to act arbitrarily, which infringes a person's right to equality before law. This is not merely an academic problem.

There is at least one prior instance in which a cyberbullying statute was struck down as unconstitutional on this ground. In *People v. Marquan M. (2014)*, [35] the New York Court of Appeals struck down a local law which had defined cyberbullying in overly broad terms. The local law in question defined cyberbullying as, "any act of communicating or causing a

---

[29] 18 U.S.C. § 1514(d)(1)(B).
[30] *Supra* note 18 at 21-31.
[31] Jessica P. Meredith, Combating Cyberbullying: Emphasizing Education over Criminalization Criminalization 63(1) Federal Communications Law Journal 311 (2010), p. no. 324.
[32] The Harmful Digital Communications Act, 2015 (Public Act No. 63 of 2015), s. 6(1) (New Zealand).
[33] *E.P. Royappa v. State of Tamil Nadu* (1974) 4 SCC 3 (India); *Masethla v. President of the Republic of South Africa* [2007] ZACC 20 (South Africa); *Kahkewistahaw First Nation v. Taypotat* [2015] 2 SCR 548 (Canada); *Shayara Bano v. Union of India* (2017) 9 SCC 1 (India).
[34] *Chintaman Rao v. State of Madhya Pradesh*, AIR 1951 SC 118; *Cox v. Louisiana*, 379 US 536 (1965); *Grayned v. City of Rockford*, 408 US 104 (1972); *Kartar Singh v. State of Punjab* (1994) 3 SCC 569 (India); *Print Media South Africa v. Minister of Home Affairs* [2012] ZACC 22 (South Africa); *Shreya Singhal v. Union of India* (2015) 2 SCC 1.
[35] *People v. Marquan M.*, 2014 WL 2931482 (Court of Appeal, New York, US).

communication to be sent by mechanical or electronic means, including posting statements on the internet or through a computer or email network, disseminating embarrassing or sexually explicit photographs; disseminating private, personal, false or sexual information, or sending hate mail, with no legitimate private, personal, or public purpose, with the intent to harass, annoy, threaten, abuse, taunt, intimidate, torment, humiliate, or otherwise inflict significant emotional harm on another person". [36] The Court found that this definition of cyberbullying can be interpreted in a "non-exhaustive list of ways" to include within its scope constitutionally protected speech. [37] Thus, the Court struck down the law as unconstitutional due to the overbreadth of this definition. [38]

Although this is a US precedent, it is very much relevant in the Indian context, since Indian courts apply the very same standard of overbreadth to strike down laws as unconstitutional. [39] The wording of this definition is also discomfitingly similar to the wording of erstwhile Section 66A of the Information Technology Act, 2000, which was struck down by the Supreme Court of India as unconstitutional on the same ground of overbreadth to the point of being unduly free speech-restrictive. [40] The *Marquan* case thus serves as a cautionary tale which warns us not to define cyberbullying in overly broad, or general, terms, lest it infringe on constitutionally protected speech.

3.2. Discovering a New Definition for Cyberbullying

We recognize that it is impossible to draft laws without absolute precision. However, the constitutional guarantee of right to equality before law requires us to draft a reasonably precise definition of cyberbullying.

In this endeavour, we take inspiration from the definition of, sexual harassment in the POSH Act, [41] and ragging in the UGC Anti-Ragging Regulations. [42] Both these definitions stand out as fairly precise expositions of precisely what broad categories of conducts qualify as sexual harassment, and ragging, respectively. The POSH Act defines with a fair degree of precision an exhaustive list of five conducts which are considered to be sexual harassment. [43] In a

[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] *Supra* note 33.
[40] *Shreya Singhal v. Union of India* (2013) 12 SCC 73 (India).
[41] The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 (Act 14 of 2013).
[42] Curbing the Menace of Ragging in Higher Educational Institutions Regulations, 2009, University Grants Commission, *The Gazette of India* (June 17, 2009).
[43] *Id.*, s. 2(n).

similar vein, the UGC Anti-Ragging Regulations defines with a fair degree of precision an exhaustive list of ten conducts which are considered to be ragging. [44] A definition of cyberbullying must be similarly drafted. It should specify exhaustively, and with a fair degree of precision, the broad categories of conducts which are considered to be cyberharassment.

Consistent with the general tendency of the law to apply an objective standard, we propose an objective, 'reasonable person' standard to determine whether cyberbullying has taken place. We refrain from conclusively defining cyberbullying in this proposal. Rather, we propose a scientific, three-stage process by which a definition of cyberbullying may be discovered:

1. In the first stage, we propose a country-wide sample survey of persons with access to the Internet. This survey is intended to locate a 'reasonable person' conception of what conducts constitute cyberbullying. Inevitably, the survey must be scientifically designed. Professional surveyors, in consultation with domain experts, must design the survey. In specific, they must determine an appropriate threshold of agreement by the survey participants, above which a particular conduct will be deemed to be cyberbullying. [45] The survey can be administered by the NSSO or the CSO. Such a survey would not be unprecedented. A sample survey conducted in the US by Pew Research Centre in 2017-18 discovered a significant consensus in the country regarding the conducts which constitute online harassment. [46] A similar exercise can be carried out in India, to discover a shared social conception of cyberbullying.

2. In the second stage, we propose a second level of scrutiny by healthcare professionals qualified to express a fair professional opinion on the harms of cyberbullying. Once again, we propose a similar sample survey of, or consultation with, this cohort of persons, to identify further conducts which should be considered cyberbullying by virtue of the significant harm they cause to the physical, or mental, health of their target.

3. In the third, and final stage, the list of conducts deemed to constitute cyberbullying by virtue of the prior two stages must be vetted on their constitutionality by a cohort of

[44] Rule 3.
[45] To use a simplistic example: if the threshold is set at 70%, and >70% of the survey participants agree that ϕ is an instance of cyberbullying, ϕ must be deemed to be a conduct which constitutes cyberbullying. Far more nuanced statistical measures than 'percentage' may also be designed for this purpose.
[46] Aaron Smith and Maeve Duggan, "Crossing the Line: What Counts as Online Harassment?", Pew Research Centre, *available at* https://www.pewresearch.org/internet/2018/01/04/crossing-the-line-what-counts-as-online-harassment/ (last visited on April 08, 2021).

domain experts qualified to express a fair professional opinion on this question. Policymakers must thus draft definitions of each of these conducts, giving to each of those conducts the fullest possible breadth consistent with them withstanding constitutional scrutiny.

The first, and second, stages should ideally be conducted independent of each other, perhaps even simultaneously, so as to ensure that the participants in either stage are not influenced by the results of the other stage. This robust, three-stage process will allow policymakers to scientifically discover a definition of cyberbullying which fairly balances the conflicting interests of protecting persons from the harms of cyberbullying vis-a-vis securing the right to freedom of speech and expression.

As a starting point for this inquiry, we propose that the following conducts can be considered an indicative list of behaviours which may amount to cyberbullying:

1. Any form of sexual harassment, voyeurism, and stalking, of the victim carried out online. In this context, 'sexual harassment', 'voyeurism', and 'stalking', have the meaning attributed to them in Section 376A of the IPC, [47] Section 66E of the IT Act, [48] and Section 354D of the IPC [49] but without any distinction as to gender. Thus, in this context, the victim of 'sexual harassment' can only be a woman, but a victim of 'voyeurism' or 'stalking' can be any person regardless of their gender.

2. Speech which has the tendency to incite a person to commit a criminal offence to the injury of the victim's person or the victim's property.

3. All forms of hate speech communicated online, and directed towards, the victim. In this context, 'hate speech' means the "advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence", [50] which is the internationally recognized definition of this concept.

4. Disclosure of the victim's private information online without their consent. In this context, 'private information' means any information in respect of which the victim has a "reasonable expectation of privacy".

[47] The Indian Penal Code, 1860 (Act 45 of 1860).
[48] The Information Technology Act, 2000 (Act 21 of 2000) (India).
[49] *Supra* note 47.
[50] The International Covenant on Civil and Political Rights, 1966, art. 20(2); Jeroen Temperman, "The International Covenant on Civil and Political Rights and the "Right to be Protected against Incitement"" 7(1) *Journal of Law, Religion, and State* 89 (2019).

5. Communicating online, any picture depicting the victim which has been edited without their consent.

6. The publication of, any information online which is defamatory to the victim.

4. Institutional Framework & Enforcement Mechanism

4.1. The Requirement of an Institutional Framework to Tackle Cyberbullying

A well-designed adjudication, and enforcement, mechanism is required to tackle the menace of cyberbullying across educational institutions. Here, we will explore how a good design can be made for a uniform, national framework to govern all educational institutions.

Earlier, in the 1990s, ragging was very much prevalent across Indian universities. In the Indian context, it is appropriate to look at institutional cyberbullying through the lens of ragging, as there are a lot of similarities for both these pressing issues. Like anti-ragging legislations enacted by Governments, it is also important for the Government to now enact anti-cyberbullying legislation. Penal laws prohibiting ragging have had some positive effects, but institutional mechanisms have been proven to be the most effective. [51]

Justifications 'defending' cyberbullying may arise [52] from students claiming that it makes them tougher and builds collegiality, which risks normalising this harmful behaviour. [53] The same happened for ragging, and the myth of 'positive' ragging still exists in India. [54] Even though there are no specific state or national laws, institutions can still effectively tackle cyberbullying by implementing in-house mechanisms, including reporting severe violations to the police for criminal action. Nevertheless, having a good institutional mechanism will be far more effective. [55] This policy can be enforced in educational institutions across India by Academic Boards (such as, CBSE, CISCE, etc.), and statutory bodies and sectoral regulators (such as, UGC, AICTE, BCI, etc.)

---

[51] Abdul Raheem Mohamed Zulfi, "A Critical Review of Legal Interventions for Combating Ragging in Sri Lankan Universities: A Case Study of South Eastern University of Sri Lanka", *available at* http://ir.lib.seu.ac.lk/handle/123456789/5314 (last visited on April 10, 2021).

[52] *See Supra* note 8.

[53] Wanda Cassidy, Margaret Jackson and Karen N. Brown, "Sticks and Stones Can Break My Bones, But How Can Pixels Hurt Me?: Students' Experiences with Cyber-Bullying" 30(4) *School Psychology International* 383 (2009).

[54] Samson S.R. Nallapu, "Students Perceptions and Feedback on Ragging in a South Indian Medical College" 7(2) *South East Asian Journal of Medical Education* 33 (2013).

[55] Good institutional mechanisms have been greatly effective in tackling ragging in universities (see Sarath Lekamwasam, et al., "Preventing ragging: outcome of an integrated programme in a medical faculty in Sri Lanka" 12(4) *Indian Journal of Medical Ethics* 227 (2015)), it is likely the same will happen with cyberbullying too.

4.2. Legislating a Higher Duty of Care to Make Institutions More Accountable for Cyberbullying

A statutory provision to hold both private, and public, institutions liable for failing to take reasonable action regarding cyberbullying can be modelled on various ragging lawsuits enforcing a higher than ordinary duty of care [56] on universities to prevent ragging. [57] An institution has a higher responsibility than an ordinary person for safety, and well being, of their students. [58]

We propose that educational institutions must, within the prescribed time period, take the actions prescribed in this policy for preventing, and in response to, incidents of cyberbullying. If they fail to do so, they will be deemed to be in breach of their duty of care in this context, for which the aggrieved persons can sue to impose civil liability on the university.

The policy will solidify the civil liability (with a higher duty of care), which in itself will be a deterrent for institutions, which will further prompt them to take measures to mitigate cyberbullying and its harms. Institutions must take preventive action, sanction instances of cyberbullying within the scope of this policy, and provide restitutive relief to victims within the scope of this policy.

4.3 The Enforcement and Relief Mechanism

We suggest two bodies to constitute a proper enforcement mechanism:

1. The Internal Committee; consisting solely of internal members; whose primary role is to prevent cyber-bullying by, promoting awareness of the issues, implementing a support structure for victims, and to aid the External Committee.

2. The External Committee; an independent body, consisting of a mix of internal and external members; for adjudicating complaints, deciding on disciplinary action, and recommending further legal action outside of the scope of this policy (such as a criminal action).

---

[56] A higher duty of care means that the institution in question will be held accountable to a higher standard of care than what is expected of an ordinary, reasonable person. For example, the standard of care a doctor owes to a patient is higher than the duty of care a civilian owes to a sick person they are caring for. The premise of this argument is, educational institutions are responsible for the safety and well being of their students, and that includes steps taken by the university in respect of cyberbullying.

[57] Neerav Srivastava, Aashish Srivastava and D. K. Srivastava, "A Million Winslows: private liability of universities for ragging in India" 19(2) *Oxford University Commonwealth Law Journal* 227 (2019).

[58] Mullins v. Pine Manor College, 449 NE 2d 331 (Massachusetts, US, 1983);

4.3.1. The Internal Committee

This will be an in-house team consisting of the following members:

1. Students representing each batch, or class, of the university will be elected by that cohort to this Committee. The number of student members will thus depend on the number of batches.

2. *Three* faculty members will be appointed by the Head of the institution.

3. The in-house Counsellor appointed by the institution.

The Committee will be headed by a faculty member to be chosen by the Head of the institution.

The duties of this Committee will be:

1. To conduct anti-cyberbullying awareness campaigns on campus, and implement the preventive mechanisms *(see below, 'Preventive Mechanisms')*.

2. To assist victims with resources to cope up with the harm resulting from cyber bullying *(see below, '4.7. Personal Reliefs to the Victim')*.

3. To implement the recommendations of the External Committee.

4. To assist the External Committee in bringing a criminal action, if that Committee so decides after adjudicating a complaint.

Preventive Mechanisms— The Committee will be responsible for enforcing the following preventive mechanisms, which are intended to have the effect of mitigating the possibility of cyberbullying taking place:

1. Every person, before joining the university as a student, faculty, an officer, or an employee, must sign an affidavit promising not to indulge in cyberbullying. [59]

2. Periodic seminars, and awareness sessions, must be conducted at least once a year. The sessions must be attended by all students, faculties, officers, and employees, of the university.

[59] This requirement is borrowed from the existing UGC Anti-Ragging Regulations: see Curbing the Menace of Ragging in Higher Educational Institutions Regulations, 2009, University Grants Commission, *The Gazette of India* (June 17, 2009).

3. Posters informing of the harms, and consequences, of cyberbullying must be affixed in visible places of the institution's premises.

4.3.2. The External Committee

Members of this body will take decisions on, the remedies to be afforded to the victim, and the sanctions to be applied to the offender.

This body must be decisionally, and functionally, independent of the institution. It will consist of a mix of internal, and external, members:

1. There will be *two* internal members, one faculty representative and one student representative, each to be elected by the Internal Committee from amongst the faculty members and the student members respectively.

2. There will be *three* external members, to be appointed by the Executive Body of the institution. The members will be, *one* mental health professional, *one* person with knowledge of, or expertise in, cyber laws, and any *one* other member who is not associated with the institution.

4.4. Why the Two-Body Enforcement Mechanism?

In tackling complaints of cyberbullying, not only speed and agility, but also securing the due process rights of the alleged offender, is important.

The Internal Committee is necessary because an adjudicator cannot immediately respond to each, and everything, that happens. Additionally, internal members, by virtue of their membership of the institution, are more likely to be well acquainted with ground realities, which makes them ideally to discharge their duties. However, we cannot have the same internal members also acting as adjudicators, as that tends to increase chances of bias and thus erodes the due process requirement. Hence, we have proposed the External Committee, a broad-based body consisted of stakeholder representatives and independent experts. [60]

Although an educational institution enjoys significant leeway in taking disciplinary action against its students, due process cannot be entirely dispensed. [61] Subjecting the offender to

[60] In constituting this body, we are inspired by the Facebook Oversight Board. The Board is a body of independent, external experts, who are responsible for deciding appeals against decisions of Facebook w.r.t. regulation of content on its platform.

[61] Warren A. Seavey, "Dismissal of Students: "Due Process"" 70(8) *Harvard Law Review* 1406 (1957); *Madera v. Board of Education*, 267 F. Supp. 356 (New York, US, 1967); *Tata Cellular v. Union of India*, (1994) 6 SCC 651.

sanctions entails civil consequences. Hence, it is essential to ensure that the adjudicatory mechanism, functions in compliance with the principles of natural justice, [62] and imposes sanctions which are proportionate in the facts of every instance. [63] If these requirements are complied with, it will be fairly easy outcomes of the adjudicatory process to withstand judicial scrutiny.

4.5. Adjudicatory Mechanism

We propose the following adjudicatory mechanism by which complaints can be adjudicated before the External Committee:

1. The aggrieved student must file a complaint to the External Committee.
2. On receipt of the complaint, the Internal Committee will, help the complainant preserve the evidence, and help them to make a formal complaint to the External Committee. The External Committee must be constituted within a week.
3. The External Committee must begin proceedings within 2 weeks of the receipt of the complaint. It must hear both the parties, conduct an independent and impartial enquiry, and recommend sanctions with reasons for the same.
4. The institution will be responsible for enforcing the sanctions imposed by the Committee. The Committee may also recommend that criminal action be initiated against the offender.

Every complaint must be filed before both the victim, and the perpetrator, cease to be students of the educational institution in question. A sample best format for the complaint to be made must be made available.

The Committee should have the powers of a civil court in respect of compelling the presence of witnesses and the ordering production of evidence. The Internal Committee will assist the Committee on request. The Committee should decide on all complaints within 60 days of the receipt of the complaint.

---

[62] The principles of natural justice apply in every case which entails civil consequences: *Maneka Gandhi v. Union of India*, AIR 1978 SC 597; *Mohinder Singh Gill v. Chief Election Commissioner*, AIR 1978 SC 851 (India). Thus, the principles will very much apply in this context.
[63] *Ranjit Thakur v. Union of India*, AIR 1987 SC 2386; *Omkumar v. Union of India*, AIR 2000 SC 3689.

4.6. Enquiry Procedure and Sanctions

The External Committee must begin its procedure within *two* weeks of receiving a complaint. The victim may appoint upto *two* members of the Internal Committee to assist them.

Proceedings will be held on record, digital evidence and history will be checked, the process will mandatorily have confidentiality. After the process, depending on the violations, sanctions can be enforced. The sanctions can include everything from an admonishment to dismissal from the institution. When an ascertained student has been found guilty of cyberbullying, it must be reflected in their conduct record document awarded at the time of passing out.

Where the conduct of the offender amounts to a specific offence under the Indian Penal Code or under any other law, and if the adjudication body finds it necessary that the particular offence must be recommended for punishment, then the respective institution will notify law enforcement to take further actions.

4.7. Personal Reliefs to the Victim

Immediately after the complaint is raised, the institution will provide a counsellor (in-house or external) to the victim to reduce the effect of the trauma suffered. There is also an option to give the victim long term counselling services by the institution to cope up with the trauma. In case the victim requests assistance to take down the harmful content, the Internal Committee must assist them.

The victim will be entitled to request for counselling at their discretion, and the Committee must provide counselling if they request for it. The costs of the counselling will be borne for the institutions. This cost burden will further act as an incentive for institutions to take measures to mitigate cyberbullying.