

Combatting Cyber- Bullying: An Analysis of Laws in India, Singapore, and Sri Lanka

Kushanthi S. Harasgama*
Hashini B. Rathnayaka**

Abstract

Technology is an inseparable aspect of modern human life. However, modern technological advancements have also exposed people to many risks of harm. Cyberbullying, i.e., the use of electronic means to intimidate, humiliate and cause distress to people, has emerged in recent times as widespread practice which can have severe negative impacts on victims. This paper examines the adequacy of existing legislation in India, Singapore, and Sri Lanka to combat cyberbullying. This analysis reveals that despite the lack of a specific law on cyberbullying, India has a range of provisions in its Information Technology Act 2000 and the Penal Code, which can capture different forms of cyberbullying. In several cases, the Indian judiciary has creatively used the provisions of these Acts to penalise cyber bullies. In Singapore, the provisions relating to harassment and cyberstalking in the Protection against Harassment Act 2014 can be utilised effectively to capture cyberbullies even though the Act does not make explicit reference to 'cyberbullying'. Sri Lanka does not have any specific laws on cyber-bullying. Some provisions of the Penal Code of 1885, Prohibition of Ragging and Other Forms of Violence in Educational Institutions Act 1998 and the Obscene Publications Ordinance 1927 can be interpreted to encompass certain forms of cyberbullying. However, they cannot cover all forms of cyberbullying, and to date, none of these laws have been used to prosecute cyberbullies in Sri Lanka. The paper concludes with a recommendation for Sri Lanka to enact a specific law on cyberbullying.

* PhD (Monash), LLM (Deakin), B.A. (Hons)(Kel'ya), Attorney-at-Law, Senior Lecturer (Higher Grade), Sri Lanka Institute of Information Technology.

** LL.B. (Colombo), Research Assistant, School of Law, Sri Lanka Institute of Information Technology.

Key Words: Cyberbullying, India, Singapore, Sri Lanka, Legislation

Introduction

Bullying, which usually involves physical or verbal abuse inflicted upon a person, is a long-standing practice among both young and elderly populations in society. The severe nature of this social phenomenon has led to a substantial body of research on causes, effects, and methods of combatting bullying in day-to-day life. However, the rapid development of technology has led to a new form of bullying often referred to as ‘cyber bullying’ or ‘online bullying’, thus adding to the traditional bullying conducted face-to-face. Cyberbullying which seems to be increasing day by day, cannot be taken lightly due to its extraterritorial nature and the complexities associated with cyberspace.

Cyberbullying can cause severe and vicious harm to victims ranging from severe mental trauma, negative impacts on physical and social well-being, to suicide. As opposed to traditional bullying, cyberbullying can take place anywhere at any time. Therefore, a victim of online bullying has no escape until the bullying is put an end to. Thus, the legislature of a country has a crucial role in combatting cyber bullying especially by enacting laws targeting this abusive online conduct.

This paper examines the laws dealing with cyberbullying in three jurisdictions, namely, India, Singapore, and Sri Lanka, to assess their adequacy in effectively combatting cyberbullying. The paper is divided into six parts; Part 1

contains the introduction while Part 2 provides an overview of cyberbullying, including its definition, prevalence, and impacts regarding existing research. Parts 3, 4 and 5 respectively discuss India, Singapore, and Sri Lanka's relevant laws and analyse their adequacy to combat cyberbullying. Part 6 concludes the paper with some recommendations.

Cyber-Bullying: Definitions, Prevalence, and Impacts

Providing a uniform definition for the term 'cyberbullying' is difficult as it has been defined in various ways in the existing literature. For instance, Bill Belsey, a Canadian educator who developed the term 'cyber-bullying describes it as 'the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others.'¹ Further expanding the above definition, Kowalski, Limber and Agatston define cyberbullying as 'the use of information and communication technologies such as email, cell phones, instant messaging, defamatory personal web sites, and defamatory online personal polling web sites, to support deliberate, repeated, and hostile behaviour by an individual or group, that is intended to harm others'.² According to Shivashankar and Rajan, cyber bullying is a form of electronic communication that harms an

¹Bill Belsey, 'Always On? Always Aware' <<http://www.cyberbullying.ca/>> accessed 03 March 2021.

²Robin Kowalski, Susan Limber and Patricia Agatston, *Cyber Bullying: Bullying in the Digital Age* (2nd edn, Wiley- Blackwell 2012) 43-57.

individual's reputation or privacy or threatens or harasses, leaving a long-lasting impact'.³ Due to advancements of technology, cyberbullying, nowadays, takes various forms such as abuse of personal information, including photos and blogs, abuse in chat rooms, impersonation, revealing confidential information, excluding someone from a chat group and exchanging rude comments continuously.⁴ Thus, cyberbullying in the modern context can be defined as using electronic means to humiliate, intimidate, or cause distress to another person.

Existing research suggests that cyberbullying has become commonplace and has been increasing since digital technologies became indispensable to daily living.⁵ The reasons for this increase include the limitless audience, more tremendous potential for anonymity by perpetrators, permanency of bullying displayed on the internet, and minimal constraints on time and space in which bullying can occur.⁶ As per the existing research cyber bullying is prevalent worldwide including in the jurisdictions

³BS Shivashankar and Aswathy Rajan 'A Critical Analysis of Cyber Bullying in India-with Special Reference to Bullying in College' (2018) 119 International Journal of Pure and Applied Mathematics <<https://ssrn.com/abstract=3554114>> accessed 13 May 2021.

⁴John O Hayward, 'Anti-Cyber Bullying Statutes: Threat to Student Free Speech' (2011) 59 Clev St L Rev 85; Thomas J Holt, Grace Chee and others, 'Exploring the Consequences of Bullying Victimization in a Sample of Singapore Youth' (2013) 23 Int'l Crim Just Rev 25.

⁵Michele L Ybarra and Kimberly J Mitchell, 'online aggressor/targets, aggressors, and targets: a comparison of associated youth characteristics' (2004) Journal of Child Psychology and Psychiatry 45.

⁶Meng-Jie Wang , Kumar Yogeeshwaran, Nadia P Andrews and others, 'How Common is Cyberbullying among Adults? Exploring Gender, Ethnic, and Age Differences in the Prevalence of Cyberbullying' (2019) Cyberpsychology Behavior and Social Networking 736.

considered in this paper. For instance, the Cyber bullying Research Centre which has collected data from more than 25,000 students across the United States since 2002, reported a victimisation rate of 33.6 % in 2018⁷. A study which analysed a sample of global studies on cyberbullying has found that estimates of prevalence ranged from 1–30% for cyberbullying perpetration and 3–72% for cyberbullying victimisation.⁸ A study conducted by Microsoft Corporation in 25 countries has revealed China (70%), Singapore (58%), and India (53%) as having the highest rates of online bullying.⁹ In Sri Lanka, too, despite the lack of exact statistical data on cyberbullying, a recent report of CERT¹⁰ indicates that around 15895 social media related incidents were reported to it in 2020 and the majority of these related to abusive conduct via Facebook.¹¹ In addition to the above, from time to time, one hears of cases of cyberbullying over the media, such as the body shaming incident of some participants of Sri Lankan ‘Comic Con Cosplay’ in 2017.¹² Posting of abusive comments and messages

⁷JW Patchin, ‘Lifetime cyberbullying victimization rates: ten different studies 2007–2016’ (Cyberbullying Research Center, 2016) <<https://cyberbullying.org/summary-of-ourcyberbullying-research>> accessed 10 May 2021.

⁸Ellen M Selkie, Jessica L Fales and Megan A Moreno, ‘Cyberbullying Prevalence among United States Middle and High School Aged Adolescents: A Systematic Review and Quality Assessment’ (2016) *J Adolesc Health* 125.

⁹Redmond Wash, ‘Online Bullying is a Top Concern among Youth’ (Microsoft news center 26 June 2012) <<https://news.microsoft.com/2012/06/26/online-bullying-is-a-top-concern-among-youth/>> accessed 10 May 2021.

¹⁰ Sri Lanka Computer Emergency Readiness Team.

¹¹The National CERT of Sri Lanka, *Annual Activity Report 2020 Sri Lanka CERT CC*

<https://cert.gov.lk/documents/Sri_Lanka_CERT_Annual_Activity_Report_2020.pdf> accessed 18 May 2021.

¹² Amalini De Sayrah , ‘On the Harassment of the Lanka Comic Con Players’

targeting particular individuals occur on social media daily. However, most of these go unreported due to the anonymity of the perpetrators, victims' lack of awareness about the available remedies and victims' fear of social stigmatisation.¹³

The severe negative impacts that cyber-bullying can have on victims are well documented in the literature. For instance, cyberbullying has been found to lead to physical and mental health problems, including anxiety, depression, suicidal tendencies, substance abuse etc.¹⁴ Studies have also found that the youth who experience cyberbullying are more likely to complain of difficulty in sleeping, recurrent abdominal pain and frequent headaches.¹⁵ Given the prevalence and the severity of the harms caused by cyberbullying, it is crucial to provide sufficient mechanisms, including laws, to combat this anti-social conduct.

Indian Laws on Cyber Bullying

Although cyberbullying has been found to be widespread in India, the country does not have any statute directly dealing with this problem. Nevertheless, some sections of the Information Technology Act 2000 (hereinafter

(Ground Views 01 September 2017)

<<https://groundviews.org/2017/09/01/on-the-harassment-of-the-lanka-comic-con-players/>> accessed 14 May 2021.

¹³Michele (n5).

¹⁴Ellen (n8).

¹⁵A Sourander, A Brunstein Klomek , M Ikonen and others, 'Psychosocial risk factors associated with cyberbullying among adolescents: a population-based study' (2010) Arch Gen Psychiatry 67.

referred to as IT Act) and The Indian Penal Code 1860 (hereinafter referred to as IPC) can be utilised to prosecute cyberbullying.

Section 66A of the IT Act, which the Indian Supreme Court struck down in *Shreya Singhal v. Union of India*¹⁶ as being unconstitutional, criminalised sending by means of a computer resource or a communication device any information that is grossly offensive, had a menacing character or is false for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will.¹⁷ Thus, anyone who sends or posts abusive, offensive, menacing or false content through emails, social media, chat rooms etc. could have been persecuted under this section. However, as mentioned above in *Shreya Singhal v. Union of India*¹⁸, the Indian Supreme Court has struck off this section in its entirety. It violated the right to freedom of expression guaranteed under Article 19(1) (a) of the Indian Constitution. Therefore, a provision that could have been used progressively to prosecute cyberbullies is no longer a part of the Indian legal system.

However, the IT Act still has some provisions which can be used to tackle various forms of cyberbullying. For

¹⁶*Shreya Singhal v. Union of India* (2015) 5 SCC 1.

¹⁷Section 66A explanation— For the purpose of this section, terms “electronic mail” and “electronic mail message” means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, images, audio, video and any other electronic record, which may be transmitted with the message.

¹⁸*Shreya Singhal* (n 15).

instance, section 66C of the said Act criminalises identity theft. It provides that whoever, fraudulently or dishonestly, uses the electronic signature, password or any other unique identification feature of any other person can be punished with imprisonment up to three years and/or a fine. Section 66D of the same Act can be utilised to persecute those who engage in impersonation.¹⁹ Furthermore, Section 66E criminalises intentionally or knowingly capturing, publishing, or transmitting the image of a private area of any person without his or her consent, under circumstances violating that person's privacy. Section 67 punishes those who publish or transmit obscene material in electronic form, while section 67A criminalises publishing, transmitting, or causing to be published or transmitted any material which contains sexually explicit act or conduct. The above provisions can be used to prosecute online bullying to a certain extent since cyber bullying can take many forms such as changing the victim's password, sending inappropriate messages to people on victim's contact list, creating fake accounts in victim's name in order to humiliate (impersonation/ masquerading), repeatedly sending cruel, insulting and harassing messages, manipulating pictures of the victim and sending to others etc.²⁰

¹⁹Whoever, by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

²⁰Susan Keith and Michelle E Martin, 'Cyber-Bullying: Creating A Culture Of Respect In A Cyber World' (2005) 13 Reclaiming Children & Youth: The Journal of Strength-based Interventions <<https://www.semanticscholar.org/paper/Cyber-Bullying%3A-Creating-a->

In addition to IT Act, some provisions of the IPC can also be construed to encompass cyberbullying. Section 354A of the IPC deals with sexual harassment against women and criminalises *inter alia* making demands for sexual favours; showing pornography against the will of a woman or making sexually coloured remarks. This provision can be construed to protect women from the harassment that takes place in the cyberspace. For instance, a cyber-bully who makes sexually coloured remarks against women such as body-shaming through vulgar comments on social media, can be prosecuted under this section.

Culture-of-Respect-in-a-Keith-Martin/84167ccc43bc7cc74b5e402702cd4cc754a6df7a> accessed 12 May 2021; Justin W Patchin and Sameer Hinduja, 'Bullies Move Beyond The Schoolyard' (2006) 4 Youth Violence and Juvenile Justice <<https://journals.sagepub.com/doi/10.1177/1541204006286288>> accessed 14 May 2021; Heidi Vandebosch and Katrien Van Cleemput, 'Defining Cyberbullying: A Qualitative Research Into The Perceptions Of Youngsters' (2008) 11(4) Cyber Psychology & Behaviour <<https://www.liebertpub.com/doi/abs/10.1089/cpb.2007.0042>> accessed 14 May 2021; Sameer Hinduja and Justin W Patchin, 'Bullying, Cyberbullying, And Suicide' (2010) 14(3) Archives of Suicide Research <<https://pubmed.ncbi.nlm.nih.gov/20658375/>> accessed 12 May 2021; Mohamed Chawki and Yassin Shazly, 'Online Sexual Harassment: Issues & Solutions' (2013) 4(2) Journal of Intellectual Property, Information Technology and E-Commerce Law <<https://www.jipitec.eu/issues/jipitec-4-2-2013/3742>> accessed 14 May 2021; Samaneh Nadali and others, 'A Review Of Cyberbullying Detection: An Overview', 13th International Conference on Intelligent Systems Design and Applications (ISDA) (IEEE 2013) <<https://ieeexplore.ieee.org/document/6920758>> accessed 14 May 2021; Vishaka S Suriyabandara, 'An Analysis Of The Attitude Towards Cyberbullying And Cyber Victimization Among The University Students Of Sri Lanka' (2017) 4 World Journal of Social Science <<http://www.sciedu.ca/journal/index.php/wjss/article/view/11314/6945>> accessed 12 May 2021.

Section 354C creates the offence of voyeurism and provides that a person who takes pictures of a woman or watches her where she expects privacy or when she is indulging in some private activity and expects no one to be observing, shall be punished with imprisonment for not less than one year and up to three years, and shall also be liable to fine under first conviction. For the second or subsequent conviction, there is imprisonment between three to seven years and a fine. Under this section, a cyber-bully can be punished for taking intimate/sexually explicit pictures of a woman without consent and disseminating such photos. Importantly subsection 2 of this provision criminalises non-consensual dissemination of intimate/sexually explicit photos which were taken with the woman's consent. For instance, if a man publishes a nude picture of his ex- girlfriend in order to seek revenge and humiliate her, he can be prosecuted under this section.

However, harassment that occurs in the cyberspace is not limited to women but also to men and LGBT community; thus, Section 354C is insufficient to provide redress to men or the transgender community, who are also the victims of cyberbullying.

Other IPC provisions that can be relevant to cyberbullying include , section 292A which criminalises, inter alia, selling, hiring, distributing, publicly exhibiting, making, producing or having in possession any obscene

material, section 499 which deals with defamation²¹, section 419 which decriminalises cheating by personation, section 503 which deals with criminal intimidation through any anonymous communication and Section 509 which punishes offenders who insult the modesty of a woman by words or gesture by intruding the privacy of the woman.

The Indian Judiciary has utilised some of the above provisions to punish cyberbullies in several instances. In the case of *State of West Bengal v. Animesh Boxi*²² the accused took possession of some private and intimate photographs of the victim by hacking into her phone, blackmailed her by threatening to upload the stolen pictures and videos on the internet, and subsequently uploaded her private pictures and intimate videos onto a porn website. Furthermore, the court commented that ‘deterrence was one of the prime considerations for convicting the accused and an inadequate sentence would do more harm than justice, as it would undermine public confidence in the seriousness of the issue.’ The Court convicted the accused under sections 354A, 354C, 354D, 509 of the Indian Penal Code and sections 66C and 66E of the IT Act, thus utilising both pieces of legislation to punish the wrongdoer.²³

Thus, Indian judicial system has utilised the existing laws

²¹This section deals with the situations when a person by spoken words or signs makes or publishes something with the intent to harm the reputation of the other person.

²²*State of West Bengal v. Animesh Boxi* [2017] CRM NO 11806.

²³*State of West Bengal* (n22).

to punish cyber bullies. However, absence of a uniform law has compelled the prosecutors to rely on multiple laws to prosecute the perpetrators; thus, creating more complexities in the legal system. Therefore, a provision on cyber bullying should either be inserted into the existing IT Act, or a uniform piece of legislation which deals with cyber bullying should be introduced to Indian legal system to tackle the matters of cyber bullying in a more robust and effective manner.

Singaporean Laws on Cyber Bullying

In Singapore, the law applicable to cyber bullying can be found in the Protection from Harassment Act (hereinafter referred to as POHA) which was enacted in 2014. Although the terms ‘cyber bullying’ or ‘bullying’ are not used in this piece of legislation, this Act has been enacted to provide both criminal and civil remedies against harassment, including online harassment. During the Second Reading of the Protection against Harassment Bill, Mr. Shanmugam, the Minister of Law emphasised that this Act would cover a wide range of anti-social behaviour, such as cyberbullying, bullying of children and sexual harassment, wherever it takes place.²⁴ Thus, it is evident that the Singaporean legislature intended to curb all forms of online harassment as well as physical harassment through the introduction of this enactment.

²⁴Singapore Parliamentary Debates Official Report 13 March 2014, vol 91.

Section 3 of the POHA which prohibits intentionally causing harassment, alarm or distress to another person by any means, section 4 which prohibits harassment, alarm or distress to another person by any means are some of the sections that can be utilised to redress victims of cyber bullying.²⁵ Prior to enactment of POHA, harassment was a criminal offence under Sections 13A–13D of Miscellaneous Offences (Public Order and Nuisance) Act 1985. However, it was not clear whether online harassment was covered under that Act. Therefore, sections 3 and 4 of POHA, re-enacted the sections 13A and 13B of the Miscellaneous Offences (Public Order and Nuisance) Act with suitable modifications to extend to words, behaviour or communication used or made by ‘any means’, including through electronic means. However, POHA does not define the word ‘harassment’, thus suggesting that this term, like the words ‘insult’ and ‘abusive’, is intended to be accorded a common sense meaning.²⁶ Courts have utilised judicial precedence to construe the meaning of harassment, to provide greater benefits to victims. In *Malcomson Nicholas Hugh Bertram v. Naresh Kumar Mehta*²⁷, the term ‘harassment’ was interpreted to mean ‘a course of conduct by a person, whether by words or action, directly or through third

²⁵Illustrations provided in section 3 & 4, such as illustration (c) of s3 and illustration (a) of s 4 refer to harassing behavior committed using websites and social media, thus further indicating the applicability of these sections to incidents of cyber bullying.

²⁶GOH Yihan and YIP Man ‘The protection from Harassment Act 2014: Legislative comment’ (2014) 26 Singapore Academy of Law Journal 700, <https://ink.library.smu.edu.sg/sol_research/1394> accessed 15 May 2021.

²⁷*Malcomson Nicholas Hugh Bertram v Naresh Kumar Mehta* [2001] 4 SLR 454.

parties, sufficiently repetitive in nature as would cause, and which he ought reasonably to know would cause, worry, emotional distress or annoyance to another person.’ In *Chee Siok Chin v. Minister for Home Affairs*²⁸ court noted that the ‘essence of harassment is not just repetitive conduct but includes prolonged or persistent or sustained conduct’ . .

Moreover, Section 5 of POHA prohibits the use of any threatening, abusive or insulting words or behaviour, or making any threatening, abusive or insulting communication to inflict fear on the victim or provoke violence, can also be utilised to prosecute cyber bullies. Furthermore, section 7 of the POHA, which prohibits cyberstalking, can also be applied to particular instances of cyberbullying. As per section 7 (3), making any communication or attempting to make any communication by any means to the victim or to a related person can amount to stalking. Illustrations to section 7 (3) further demonstrate that the acts such as Y repeatedly sending emails to Y’s subordinate X with suggestive comments about X’s body, Y repeatedly circulating revealing photographs of classmate X to other classmates are punishable offences under the POHA.

Since the Act came into force in 2014, several individuals have been prosecuted and convicted for engaging in harassing activities using the internet. For instance, in

²⁸*Chee Siok Chin v Minister for Home Affairs* [2006] 1 SLR(R) 58.

*Public Prosecutor v. Ng Wei Long*²⁹ the accused was charged under section 7 of POHA for sending sexually explicit messages via social media platforms and text messages to the victim. Moreover, in *Public Prosecutor v. Lai Zhi Heng*³⁰, the defendant, who uploaded nude photographs of the victim onto the Facebook group of her school friends with the false message that she was offering prostitution services, was found guilty and sentenced for six months imprisonment under section 7. Therefore, it is important to note that section 7 of POHA is a powerful section which can be used not only against those who engage in stalking as it is traditionally understood, but also in other bullying or harassing conduct via the internet.

Cyber Bullying Laws in Sri Lanka

Careful consideration of the existing laws in Sri Lanka reveals that there is no uniform or specific legislation to deal with cyberbullying in the country. However, a few provisions of the Penal Code Act of 1885, Obscene Publication Ordinance No.4 of 1927 and the Prohibition of Ragging and Other Forms of Violence in Educational Institutions Act No. 20 of 1998 (hereinafter referred to as Anti-Ragging Act) can be utilised to prosecute cases of cyberbullying. It is important to note here that the provisions of Computer Crimes Act No.24 of 2007 are insufficient to prosecute cyber bullying as the offences created by the said act are limited to crimes where

²⁹*Public Prosecutor v Ng Wei Long* [2019] SGMC 78.

³⁰*Public Prosecutor v Lai Zhi Heng* [2019] SGHC 99.

computers are utilised for criminal activities such as fraud, theft, hacking and similar conduct.

Section 345 of the Penal Code provides that whoever by assault or use of criminal force sexually harasses another or uses words or actions cause sexual annoyance or harassment to such other person commits the offence of sexual harassment. Since cyber bullying involves harassing a person by using threatening words or actions, it can be argued that cyberbullying falls within the purview of this section. Therefore, a victim who has been subjected to sexually coloured remarks in social media may utilise this section to prosecute the perpetrators. However, as this section only covers gender-based harassment, it cannot be used in cyberbullying cases involving religion, race and ethnicity.

Furthermore, Section 483 of the Penal Code creates the offence of criminal intimidation. It provides that 'whoever threatens another with injury to their person, reputation or property, or to the person or reputation of anyone whom that person is interested in, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intimidation'. Again, this provision appears to be broad enough to cover cyber bullying cases involving threats of harm to the victim's person, property, and reputation. For instance, a cyberbully who threatens to beat up the victim

or threatens to publish sharp images of a victim online can potentially be captured under this provision.

Section 2 of the Anti-Ragging Act is another provision that can be used to prosecute cyberbullies. It prohibits ragging, defined in section 17 of the same Act as ‘any act which causes or is likely to cause physical or psychological injury or mental pain or fear to a student or a member of the staff of an educational institution.’ Since the section refers to ‘any act’ likely to cause physical, psychological injury, mental pain, or fear, it has the potential to encompass any form of cyberbullying such as sending threatening/insulting/abusive messages to the victim, posting insulting comments about a victim on social media, posting/sharing sensitive images/videos of a victim on social media or a website or in a chat group. However, as the applicability of the Anti-Ragging Act is limited to educational institutions, it does not provide redress to victims of cyberbullying outside educational institutions.

Section 2 of the Obscene Publication Ordinance No.4 of 1927 is a provision that can potentially be used to prosecute cyberbullying to a certain extent. Section 2 criminalises, *inter alia*, the acts of making, producing or having in possession for distribution or publicly exhibiting obscene material. Therefore, an individual who makes produces or possesses nude or sexually explicit images/videos of a victim to publicly exhibit or distribute such material via online platforms. Thus, bullying a victim can be prosecuted under this section.

Thus, it is evident from the above discussion that Sri Lanka too has some criminal laws that can potentially be used to prosecute cyberbullies. However, such laws make no explicit reference to cyberbullying. Unfortunately, due to the lack of awareness among law enforcement authorities on the applicability of these laws to online misconduct and lack of judicial activism in this area, victims of cyberbullying in Sri Lanka suffer without any legal redress. In contrast, cyberbullies continue their malicious activities without any punishment. It is also important to note that despite their potential to encompass some instances of cyberbullying and harassment, existing laws are insufficient to cover all types of cyberbullying and harassment. Thus, the country needs a robust set of specific laws on cyberbullying and harassment. Such a law should focus not only on penalising perpetrators but also on providing adequate assistance to victims to overcome the trauma they've experienced as a result of cyberbullying. Legislation that punishes perpetrators while providing civil remedies for victims like the POHA of Singapore would go a long way in addressing cyberbullying and harassment.

Conclusion

Technology is a double-edged weapon that has both advantages and disadvantages. In this digital era, it is difficult to survive without the aid of electronic means. Especially during this Covid-19 pandemic situation, it was the technology that kept us connected and facilitated

education, work, etc. However, technology has also made us more vulnerable and exposed us to risks of criminal activities, including cyberbullying and harassment.

This paper analysed the adequacy of the laws in three jurisdictions, namely, India, Singapore and Sri Lanka, in combatting cyberbullying. This analysis reveals that despite the lack of a specific law on cyberbullying, India has a range of provisions in its IT Act and the Penal Code that can capture different forms of cyberbullying. In several cases, the Indian judiciary has creatively used the provisions of these Acts to penalise cyber bullies. In Singapore, the provisions relating to harassment and cyberstalking in the recently enacted Protection against Harassment Act 2014 can be utilised effectively to capture cyberbullies even though the Act does not explicitly reference 'cyber bullying'. Provisions of this Act have been used to prosecute and convict several individuals who have engaged in different forms of cyberbullying and harassment. Sri Lanka, on the other hand, does not have any specific law on cyber-bullying. However, some provisions of the Penal Code, Anti-Ragging Act and the Obscene Publications Ordinance can be interpreted to encompass certain forms of cyberbullying, if not all. However, to date none of these laws have been used to prosecute cyber bullies. Thus, it is recommended for Sri Lanka to enact a robust law on cyber bullying that facilitates punishment of cyber bullies and provides effective redress to victims such as assistance to recover from the trauma and harms suffered at the hands of cyber bullies and compensation.