



INTERNATIONAL JOURNAL OF LAW,
GOVERNMENT AND COMMUNICATION
(IJLGC)
www.ijlgc.com



BRIDGING THE GAPS IN MALAYSIA'S CYBERBULLYING LAWS: CHALLENGES AND REFORM PROPOSALS

Arina Kamarudin¹, Irma Kamarudin^{2*}, Siti Khadijah Abdullah Sanek³

¹ School of Law, NMUC (Netherlands Maritime University College), Malaysia
Email: arina@nmuc.edu.my

² Department of Law, Universiti Teknologi MARA Kedah Branch, Malaysia
Email: irma@uitm.edu.my

³ Department of Law, Universiti Teknologi MARA Kedah Branch, Malaysia
Email: khadijah016@uitm.edu.my

* Corresponding Author

Article Info:

Article history:

Received date: 05.01.2025

Revised date: 18.01.2025

Accepted date: 25.02.2025

Published date: 10.03.2025

To cite this document:

Kamarudin, A., Kamarudin, I., & Abdullah Sanek, S. K. (2025). Bridging the Gaps in Malaysia's Cyberbullying Laws: Challenges and Reform Proposals. *International Journal of Law, Government and Communication*, 10 (39), 133-147.

DOI: 10.35631/IJLGC.1039008

This work is licensed under [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/)



Abstract:

Cyberbullying has become an increasingly prevalent issue in Malaysia, exacerbated by the widespread use of digital communication platforms and social media. This article critically examines the existing legal framework governing cyberbullying in Malaysia, with particular attention to the Communications and Multimedia Act 1998, the Penal Code, and the Defamation Act. It evaluates the extent to which these legal provisions effectively protect victims and ensure accountability for perpetrators. Furthermore, this study explores key challenges in the enforcement of cyberbullying laws, including jurisdictional complexities, the anonymity of offenders, and limitations in public awareness and legal literacy. Despite the presence of legal mechanisms, gaps remain in legislative scope, enforcement capabilities, and preventive measures. The article argues for a more comprehensive and victim-centered legal approach, incorporating stricter enforcement, policy reforms, and enhanced digital literacy initiatives to address the evolving nature of cyberbullying. The findings underscore the need for a multi-stakeholder strategy involving legal, technological, and educational interventions to strengthen Malaysia's legal protection against online harassment.

Keywords:

Abuse – Cyberbullying – Digital Enforcement – Online Harassment – Policy Reforms – Social Media

Introduction

The heartbreaking story of Esha Rajeshwary Appahu brings to light the devastating effects of cyberbullying in Malaysia. Her experience has sparked nationwide awareness about the dangers of online harassment and its potential to result in tragic consequences, further emphasizing the urgent need for comprehensive legal responses to combat such behaviour. (Sipalan, 2023). As a prominent young TikTok influencer, Esha's situation illustrates the profound and widespread implications of cyberbullying in our society. Enduring persistent harassment on various platforms, her case reveals how contemporary technology can intensify the struggles of at-risk individuals, particularly young people who often lack the means to cope with such torment effectively. (Qazi & Hamid, 2023)

Cyberbullying utilizes social media, blogs, and messaging apps, creating a facade of anonymity that allows bullies to intimidate and torment their victims without facing repercussions. (Barlett et al., 2018) In Esha's situation, her tormentors went to the extent of spreading harmful and damaging rumours about her, severely impacting her mental health and overall well-being. (Channel News Asia, 2024) Ultimately, this continuous campaign of abuse led to her tragic decision to take her own life, starkly illustrating the deep emotional anguish that arises from such merciless cruelty. Regrettably, the bullies responsible for this behaviour faced little to no consequences (Channel News Asia, 2024), highlighting a significant gap in accountability and raising serious concerns regarding the effectiveness of existing measures to protect against harassment in Malaysia. This distressing scenario prompts urgent discussions about how society addresses cyberbullying, stressing the necessity for systemic changes that can offer better protection for individuals confronting this widespread threat that affects countless young lives. (Falla et al., 2021)

The primary objective of this paper is to analyze the various laws that pertain to cyberbullying within the Malaysian context and to evaluate the effectiveness of these existing legal frameworks in addressing and combating the occurrence of cyberbullying incidents. Additionally, this research will highlight the deficiencies in the current legal and policy frameworks, assess the effectiveness of existing strategies, and propose essential reforms aimed at bolstering protections against the pervasive threat of cyberbullying. To achieve this, the research employs a qualitative research methodology, which necessitates the systematic collection of pertinent information from a variety of sources. Initial results indicate that, as it stands, there is no specific legal enactment or statute within Malaysia that distinctly categorizes cyberbullying as an offence in its own right; however, it is important to note that such acts do fall under the purview of regulations specified in the Communications and Multimedia Act. The comprehensive study further revealed that the laws concerning cyberbullying require greater specificity and effectiveness in their application. Thus, it is strongly suggested that the current legal frameworks related to cyberbullying in Malaysia be seamlessly integrated into the nation's Penal Code. This integration should include the development of specific and detailed provisions addressing cyberbullying to enhance the overall effectiveness of legal recourse against such harmful behaviours.

Literature Review

Definition and Forms of Cyberbullying

"Bullying" is described as "intentional, repeated, negative (unpleasant or hurtful) behaviour by one or more persons directed against a person who has difficulty defending himself or herself."

(Olweus, 1994) More broadly, it encompasses the behaviour of offending or intimidating someone smaller or younger than you, which can occur in various contexts. (Salmivalli et al., 2021).

Bullying has emerged as a critical and pressing universal social issue, and it is increasingly recognized as an alarming global problem. (Shetgiri, 2013) Traditional forms of bullying typically involve actions that are punishable under criminal law, while the more modern phenomenon of cyberbullying involves actions carried out through the use of electronic devices. (Patchin & Hinduja, 2011) This shift not only alters the dynamics of victimization but also raises complex legal challenges. (Shukor and Osman2022) Cyberbullying can take many forms, including harassment through social media platforms, sending threatening emails, or spreading malicious rumours online. (Xu and Trzaskawka2021) (Ismail et al.2022) Unlike traditional bullying, it can occur at any time and may be perpetrated anonymously, making it difficult for victims to seek help. (Yu & Riddle, 2022) However, the term "cyberbullying" generally refers to a myriad of actions or comments that are conveyed electronically, often through digital means such as social media or messaging platforms. (Verma et al.2023) (Noor and Hamid, 2021) This particular form of behaviour can, unfortunately, manifest in numerous and diverse ways, including both verbal and written threats, as well as physical intimidation, cruel taunts, or even more persistent and damaging forms of harassment such as cyberstalking that can invade a person's online life and privacy. (Fernanda and Carla, 2023)

Cyberbullying or cyberharassment presents itself in several specific forms, which include but are not limited to flaming, harassment, cyberstalking, denigration, masquerading as another person, outing individuals publicly, engaging in happy slapping, and the sharing of explicit content, also known as sexting. (Scheithauer et al.2021) It has become apparent that greater attention needs to be devoted to regulating cyberbullying activities. (Szoka & Thierer, 2009; Langos, 2014; Ahmad Razali et al., 2022) This is essential to facilitate the continued development of the electronic environment as we move toward a knowledge-based economy. Therefore, enhancing existing cyber laws to provide better regulation of cyber activities and practices is currently under consideration and is necessary to protect individuals in this digital age.

In addition, in today's fast-paced and interconnected world, the Internet is widely utilized as a powerful means of spreading not only information but also pervasive hate material. (Foxman & Wolf, 2013; DePaula et al., 2018) This includes a variety of harmful actions such as insults, threats, slander, and numerous accusations made publicly through various channels, such as telephone communication, social media platforms, the Internet, or other forms of media. (Cinelli et al.2021) Given this alarming and dangerous growth of cyberbullying and various criminal activities conducted online, it becomes increasingly important to address the need for effective protection and to ensure the safety of Internet users everywhere. (Windisch et al.2022) The main objective is to thoroughly examine the effectiveness of the existing cyber laws and regulations in place. This examination aims to ascertain whether these laws are sufficient and clear enough to properly regulate and control the rapid expansion and increase of cyberbullying activities witnessed today. If it is determined that the current laws and regulations are inadequate in protecting users, there will be a pressing need to strengthen the existing frameworks. This effort is essential to foster a healthy, vibrant, and sound electronic environment. We should strive for better management and enhanced control over the use of

electronic devices, ensuring that all individuals can navigate the online landscape safely and responsibly.

Impact and Consequences

The impact of cyberbullying is far greater, wider, and more intimidating and may lead to death. An individual generally experiences these types of harassment through the spread of vulgar comments that can make individuals easily give up. (Ardiyani & Muhdi, 2021) Typically, casualties do not often realize that their actions have led to self-destruction. This condition is usually seen through the attitude of a victim neglecting the matter and pretending to face the bitter reality. (Nazrul et al.2023) The issue of cyberbullying becomes increasingly pressing when there are adverse consequences of this practice. In the context of the pressing issue of cyberbullying, the detrimental effects it has on victims in terms of handling stress and emotional turmoil are undeniable. Victims often find themselves grappling with overwhelming feelings due to the abusive actions inflicted upon them through various forms of communication over the internet. (Krešić Ćorić & Kaštelan, 2020) Such behaviour can certainly be considered cowardly acts on the part of the perpetrators, who choose to hide behind a screen rather than confront their victims face-to-face. In Malaysia, a notable instance marked the emergence of this troubling trend; the very first case of cyberbullying via SMS was reported in the state of Terengganu and involved a group of students from a secondary school. (Suhana, Intan, et al., 2021) This incident highlights the serious repercussions that can stem from such harassment. The psychological toll was so severe that the victims were compelled to seek medical treatment in a hospital after losing control of their emotions following the distressing SMS insults sent by a male student. (Suhana, Intan, et al., 2021)

Tragically, there have been documented cases where victims, overwhelmed by despair and unable to regulate their feelings, took the irreversible step of ending their own lives, believing this was the only escape from their pain. (C. Mawardah et al). The alarming increase in these types of distressing behaviours underscores a critical need for the introduction of comprehensive laws or specific regulations aimed at effectively addressing the issue of cyberbullying.

Such legal measures are essential not only to mitigate the harm inflicted upon victims but also to prevent the further proliferation of these adverse consequences within society. The concerning issue of cyberbullying, particularly as it manifests among students in secondary schools, warrants immediate attention and a robust response from a multidisciplinary group. (El Asam & Samara, 2016) Moreover, it is imperative that any legislation intended to tackle these matters is crafted with considerable detail and precision to ensure it accurately addresses the complexities and nuances of cyberbullying in the digital age.

Methodology

The methodology utilized is exclusively qualitative, employing standard documentation techniques and integrating a systematic analysis of philosophical viewpoints inside academia. This study relies on the analysis of library-sourced resources rather than empirical evidence. Secondary data encompasses books, references, journals, and written materials related to Cyberbullying in Malaysia and other nations. The data underwent evaluation by content analysis. Consequently, this study utilizes standard documentation research methods to obtain results on the specified topic.

The research relies exclusively on qualitative studies to explore various legal dimensions, specifically focusing on illegal uses of communication facilities and telecommunications-related offenses within the Penal Code. This approach helps to deepen the understanding of public perception, which is further enhanced by referencing older articles and data. The inclusion of these older sources is intentional; they provide historical context and a foundation for ongoing discussions in the field. Moreover, the insights contained within these earlier works often remain relevant and can illuminate contemporary issues, making them valuable for a comprehensive analysis. By utilizing qualitative studies in conjunction with these established resources, the research enables a multifaceted exploration of diverse perspectives, allowing participants to articulate their lived experiences. This inductive reasoning approach facilitates a rich tapestry of viewpoints and nuances that quantitative methods may not fully capture, ultimately enriching the overall findings and enhancing the depth of understanding in this area of study.

Results and Discussion

Legal Framework in Malaysia

In this discussion, we examine three legal frameworks that address digital harassment and cyberbullying in Malaysia. Firstly, although certain internet-related laws may encompass ancillary issues such as cybercrime, they fall short of providing adequate protection against these forms of abuse. Data protection regulations primarily focus on organizational responsibilities rather than safeguarding individual victims. Secondly, while the civil tort and the Penal Code appear promising in theory, their applicability to incidents of digital harassment is relatively recent, and significant challenges remain in their enforcement. Currently, various stakeholders, including government agencies, enforcement units, and non-governmental organizations, are actively engaged in efforts to combat cyberbullying. (Zainudin et al., 2016; Khan et al., 2020; Ahmad Razali et al., 2022). Furthermore, there is a critical need for comprehensive literature to support and enhance these initiatives. (Abd Aziz et al., 2022; Ahmad Razali et al., 2022)

The phenomena of cyberbullying and cyber harassment pose considerable challenges within the Malaysian context. Despite notable advancements in public communication technologies and the increasing prevalence of issues surrounding online interactions, the existing legal principles associated with online defamation and threats have remained largely intact. (Mahmood et al., 2018) They continue to serve as the foundational premise from which the social and legal concerns aimed at protecting individuals from anonymous acts of defamation or threats to their dignity are critically scrutinized and evaluated. Interestingly, the specific term 'cyberbullying' is not recognized within the legal statutes. (Abd Aziz et al., 2022; Ahmad Razali et al., 2022) Nonetheless, the underlying concept of bullying itself is widely acknowledged as morally wrong and inherently subjective.

The central aim of this discourse is to critically examine the multifaceted legal protections against cyberbullying within the Malaysian jurisdiction, encompassing civil, criminal, and specific regulations designed to safeguard minors. It is argued that a holistic strategy towards internet safety, which inclusively addresses individuals of all ages, ought to be embraced by Malaysian legislators. Such a strategy must entail the formulation of national legislation that thoroughly delineates and addresses every facet of cyberbullying. Current legal definitions concerning cyberbullying necessitate expansion to adequately capture instances of bullying

across diverse information and communication technology platforms. Moreover, the imposition of stringent penalties could potentially act as a formidable deterrent against the proliferation of cyberbullying behaviours.

Consequently, both criminal and civil statutes must be enforced with efficacy, ensuring that these laws incorporate unambiguous and comprehensive definitions and provisions pertinent to cyberbullying and digital abuse, without reliance on convoluted indirect associations that may foster ambiguity. The shortcomings of previous legislative measures can frequently be traced back to vague definitions. Thus, the urgent need for robust legislation that comprehensively addresses every manifestation of digital abuse is both necessary and relevant in contemporary society. While certain aspects of these legal frameworks have been deliberated in academic and public discourses, a myriad of challenges and contentions continue to obstruct their practical application, underscoring an immediate necessity for effective interventions aimed at cultivating a safer online landscape.

Existing Laws and Regulations

In scrutinizing the current laws that regulate the pressing issue of cyberbullying in Malaysia, this paper includes a succinct section devoted to examining the existing education laws alongside the cyber laws that have been put in place to address and control cyberbullying behaviour in the Malaysian context. It is the aim of this paper is to illuminate the Malaysian government's evident failure to enact specific and targeted laws designed explicitly to regulate and manage the various issues related to cyberbullying. As a clear indication of the Malaysian government's lack of a comprehensive and robust effort to effectively grapple with the ever-increasing issue of cyberbullying and its ramifications, the existing laws currently in place are not perceived as addressing the problem in a meaningful or effective manner. Moreover, it is worth noting that the educational laws present today can be considered the most anachronistic and outdated when it comes to regulating and managing cyberbullying behaviour among students in Malaysia. Initially, the bullying behaviour that occurred between students within the school environment was regulated under the framework of the Education Act, which reflected the approach taken to tackle the issue.

The terms and concepts for cyberbullying, bullying, and harassment are not recognized as stand-alone concepts in Malaysia's legislation. It may be argued that as an alternative to a stand-alone law, rather than a statute related to bullying, the legal response to anti-cyberbullying in Malaysia can be found across a range of overlapping civil and criminal laws, including civil trespass, harassment, defamation, and neglect. One of the cases of cyberbullying is cyber-harassment, which is considered an offence under Malaysian law and subject to penalties under the existing laws and regulations in Malaysia. The following will be a brief evaluation of each of these laws in light of the legal response to cyberbullying.

Relevant Sections in the Penal Code

The Penal Code is a fundamental legal framework addressing offences such as malice, insults, violence, blackmail, criminal defamation, and both verbal and physical assault. It encompasses the prohibition of disseminating false information through various means of communication, including digital and online platforms, thus safeguarding individuals' digital security, specifically pertaining to cyber defamation laws. These laws do not supersede the Penal Code; rather, they focus on prohibiting online and computer-based defamation and establishing necessary penalties for acts of cyberbullying. This legislation plays a crucial role in addressing

incidents of bullying that occur in digital environments and on social media. Given the sensitivity surrounding privacy and personal safety, the Act ensures that victims can maintain confidentiality regarding their experiences of bullying, thereby affording them necessary protection under this legal framework.

It does not deal specifically with the facts or manifestations of cyberbullying, but part of it relates to cyberbullying. If convicted, the guilty person may be sentenced to imprisonment for up to 10 to 15 years with whipping. These laws overlap only with punishment, with the body dealing with the issue unchanged. Whether the legislation in place is an effective tool to deal with this offence, the lack of comprehensive legislation that exclusively and specifically deals with cyberbullying will lead to the inability to precisely prescribe what amounts to cyberbullying and the difficulties for enforcement officers to monitor and curb cyberbullying cases effectively. This will lead to the predominant notion that cyberbullying is a minor issue and, therefore, victims are not afforded the justice they deserve. However, the lack of jurisdiction could be detrimental to the victims of cyberbullying as it may give people the illusion that torturing others online is perfectly legal and not a serious crime. The laws today are not comprehensive and specific enough to tackle the issue of cyberbullying thoroughly. The law should be constantly evolving and adapting to technology, and this could ensure justice for cyberbullying victims.

The Penal Code contains several sections relevant to the development of cybercrime laws in Malaysia, particularly concerning cyberbullying. These include Section 345, which addresses intimidation; Section 503, focusing on criminal intimidation; Section 504, which deals with intentional insult with intent to provoke a breach of the peace; Section 505, concerning statements conducing to public mischief; Section 506, which outlines punishment for criminal intimidation; Section 507, addressing criminal intimidation by an anonymous person; Section 507A, dealing with punishment for the same; Section 507B, which pertains to attempts to cause terror; and Section 509, which highlights the act of insult with intent to provoke. Collectively, these sections provide a framework for addressing various aspects of cyberbullying and will serve as a foundation for formulating comprehensive laws targeting cybercrime in Malaysia.

Analysis of Cyber Bullying Legislation and Implications

The existence of a legal framework to address the issue of cyberbullying is an indispensable ingredient for protecting individuals from cyberbullying victimization. Countries all over the world are cognizant of cyberbullying as a social ill that needs to be tackled through laws or other means possible. Why is the existence of cyberbullying laws indispensable? Proponents say that laws play a pivotal role in guiding the public at large on what is right to do and what is not. Cyberbullying, disturbing antisocial behaviour perpetrated by an individual on a victim, when enacted into laws, allows the law to discuss its necessity, its intentions, liabilities for perpetrating them, and the consequences of complying or not complying with the existence of the laws. These are useful means to explain and take preemptive steps to deter antisocial behaviour from happening on the cyber platform.

There is currently no dedicated Cyberbullying Act in Malaysia. Cyberbullying, as generally understood, refers to the act of using digital platforms and communication technologies to intentionally harm others in a way that is aggressive, hostile, and humiliating. This behaviour typically involves individuals targeting others, including minors, but without specific legal provisions, there is a lack of clear accountability for such actions. Unlike other countries, Malaysia does not have a law that specifically addresses the unique dynamics of cyberbullying,

particularly concerning children under the age of 18. To hold someone accountable, it would need to be demonstrated that the perpetrator had awareness of the victim's age and intended to cause distress or harm.

Additionally, while there is the Child Act 2001 in Malaysia, aims to protect children from neglect, abuse, and exploitation, it does not specifically encompass cyberbullying as a defined offence. The Child Act prioritizes the welfare of children and establishes protective measures, but the absence of a Cyberbullying Act leaves a gap in legal protection against digital harassment. There are provisions under the Child Act for a Child Registry, which keep track of cases of child abuse and exploitation, including details of incidents affecting children's well-being, yet it lacks the comprehensive framework needed to tackle the issue of cyberbullying effectively.

Communications and Multimedia Act 1998

Communications and Multimedia Act 1998 (Act 588) The main function of CMA 1998 is to oversee, develop, correct, and control the implementation of all activities in the field of communications and multimedia, including postings on the Internet as well as social media. Initially, the government underscored that CMA was designed as a comprehensive legislation that allows the posting of immoral content to be considered for a penalty. However, as the Information Age advances, CMA has made the government wary of matters that could disrupt harmony and stability.

The amendments made to CMA 1998 came into force on 31 August 2006. Before that, there were many controversial provisions in the act, including Sections 233 and 263. Section 233 penalizes misuse of network facilities with a two-year jail sentence a maximum fine, or both. The amendment to Section 233 emphasizes the right to freedom of speech, and therefore excuses network providers from any criminal intentions of their users, thus including those who provide network services, facilities, or content services with a stated reminder or knowledge that a publication would contravene this section. Internet cafes contravene Section 233, and a cybercafe operator could also be made bankrupt because of the block of laws. It is argued that honesty and technology, as well as the fact that technology is ready for use, require the malicious use of illegally uploaded files to be addressed. According to law, the government should take responsibility for any failure in the system. Furthermore, it shows that a good piece of legislation is the way to protect the safety of users who are generally required on the Internet. On the other side, the protective umbrella of the provision also protects the technology or service provider corporate community from violations that may cause financial harm to the party concerned.

The Personal Data Protection (Amendment) Act 2024

The Personal Data Protection (Amendment) Act 2024 (PDPA Amendment) updates and enhances the original Personal Data Protection Act of 2010. It aims to further safeguard individuals' personal data and to refine the regulations surrounding the processing of such data. In Malaysia, personal data encompasses various types of information involved in commercial transactions, including an individual's name, address, and professional interests. The term "processing" is broadly defined and includes activities such as recording, organizing, storing, adapting, altering, retrieving, consulting, using, disclosing, transmitting, and destroying personal data.

While the original PDPA focused on personal data protection, the amendments introduce stronger measures to address sensitive information, extending protections to aspects like the display and management of children's photographs. As the first piece of data protection legislation in Malaysia, the PDPA Amendment reflects a comprehensive approach to privacy, balancing both data security and access. Introduced in 2024, the amendments build on the initial framework table outlines Malaysia's Personal Data Protection Act 2010. It specifies legal grounds for excluding personal data, such as exercising legal rights, compliance with laws, emergency tracking, and research purposes. Data users have the right to access and rectify personal information and must respond to written requests within twenty-one days. The primary aim of PDPA 2010 is to safeguard individual personal data and regulate its processing within Malaysia, while also addressing data handling abroad. The act does not apply to the Federal or State Government or their agencies. Contracts involving personal data processing can be authorized on behalf of the responsible entity, and the relevant department can provide advice on these matters. The act is administered by a Minister, who holds the authority to enact regulations, which are subject to parliamentary approval. The authority to publish personal information does not apply to minors.

Challenges and Limitations of Current Laws

The absence of comprehensive cyberbullying legislation has resulted in challenges. Currently, Malaysians are reliant on traditional laws such as the Penal Code, the Communications and Multimedia Act, and the Child Act. When the penal laws were designed, they were intended to tackle and address physical harm and injury-causing behaviours. In considering how to address the challenges of cyberbullying, we should not just be utilizing the current punishments under the penal law and administering justice behind judgment.

In Malaysia, the substantial majority of discussions surrounding cyberbullying legislation have primarily centered on proposals rooted in advocacy put forth by various civil society organizations and prominent academics, aiming to pass a comprehensive Anti-Stalking Law. Furthermore, there is significant interest shown by Members of Parliament in inserting a specific clause that would criminalize both cyberbullying and stalking within the framework of the new Independent Police Complaints and Misconduct Commission Bill. Despite the absence of thorough and targeted legislation that specifically addresses the issue of cyberbullying, it is noteworthy that both civil society organizations and law enforcement are actively taking meaningful steps to confront cyberbullying challenges in Malaysia. The rising number of reported cases highlights the severity of the problem, as evidenced by alarming statistics compiled by the police alongside impactful interviews conducted with community members, respective Members of Parliament, and dedicated grassroots NGOs working tirelessly to address this issue.

Enforcement Challenges

The lack of resources available to enforcement agencies is often cited as an enforcement challenge. (Rasli, Manaf, & Ismail, 2018; Khan et al., 2020; Ahmad Razali et.al, 2020) Anecdotal evidence has shown that crime reporting within police departments is compartmentalized, with most of the resources focused on more basic cybercrime-related issues such as e-commerce scams and fraud. (Jayabalan et al., 2014; Mohamad, Ismail, & Thani, 2023) More sophisticated profile offences, such as cyberbullying and cyberstalking, are often given lesser priority.

The punishment given to the individual who drove Esha to suicide is shockingly inadequate, amounting to little more than a slap on the wrist after their role in such a tragic event. (Channel News Asia, 2024) Victims of cyberbullying, like Esha, often face stigma and discrimination when they attempt to report these offences to a police force that frequently underestimates the severity of cybercrimes. This perception of minor repercussions hampers the pursuit of justice for victims, contributing to a lack of resources and resulting in delays and backlogs while processing digital evidence against those accused. (Ahmad Razali et al., 2022) Furthermore, identifying the individuals behind anonymous online accounts presents a significant challenge, especially when they are located in different jurisdictions, leading to prolonged waits for essential data. The rapidly evolving landscape of cyber offences complicates matters further, as crimes utilizing the latest technologies emerge before law enforcement has the chance to adapt effectively. (Westmoreland & Kent, 2015) Consequently, the police often find themselves struggling to keep pace. Online spaces can feel lawless, with perpetrators typically holding the upper hand over their victims. Expanding relevant online legislation could offer more viable solutions to combat these crimes and secure justice for victims like Esha. Additionally, enhancing police powers and resources to address these issues will help reduce stigmatization and underreporting, ultimately fostering a safer online environment for everyone. (Wilson, 2020)

In Malaysia, various law enforcement agencies have been given the authority to investigate cyberbullying complaints. (Ahmad Razali et al., 2022) The major enforcers are the Malaysian Communications and Multimedia Commission and local police personnel. These two agencies are the main partners who work effectively to investigate, monitor, and impose laws in this domain. The Council of Anti Cyber-Bullying Malaysia has reiterated its difficulties with the limited resources, understanding, and authority of the Commission and the police. The Commission, through the enforcement division, is responsible for investigating and taking action against any offences that may have occurred. It is empowered to initiate investigations into any reports of a mandatory nature or on complaints from consumers or in the course of the Commission's investigation. The Commission may also, on its own, initiate an investigation into any offence that comes to its attention. Reports on activities and actions taken or enforcement and investigation can be found in the annual reports and consumer fulfilment index reports. There is a suggestion that the Commission provides an outline of either the investigation process or the number of cyberbullying complaints made each year.

Preliminary observations underscore a pressing need for comprehensive training programs tailored to equip law enforcement officials with the requisite knowledge and proficiency to navigate the ever-evolving landscape of cyber threats. Consequently, it is imperative to advocate for a systemic overhaul of the training paradigms currently in place, thereby ensuring that law enforcement agencies are adequately prepared to confront the unique challenges posed by the digital age. (McKoy, 2021; De et al, 2021) Such enhancements in training and operational capability are vital to fostering a more robust and effective response to the intricacies of cyber-related incidents.

Resource Constraint

Quite often in real cyberbullying cases, there are several constraints of resources such as funding, manpower, and technology to deal effectively with criminal investigations of stalkers or bullies who do their dirty deeds while hiding behind the computer. It has been shown that digital investigation support is required by the Royal Malaysian Police forces. (Reuters, 2024)

Some cybercriminals have particular expertise that has surpassed the Royal Malaysian Police's skill levels of digital capabilities when it's often day-to-day work. Thus, training is imperative and necessary to avoid any deficit of new officers who are often recruited into the respective police forces in charge across the country. It requires redefining the required cyber expertise, as demanded by law enforcement agencies across many other countries, which is mirrored by the Internet divisions arriving in large capacity without the necessary cybercrime experience and expertise. Therefore, recruiting police officers with a specific cyber systematic strategy is essential. Estimations can only be made by looking at the demands of experience and professional competence in other law enforcement agencies. Throughout the process, coordination is necessary so that cybercrime capability can adjust efficiently and effectively according to the digital law enforcement officers against the actual numbers of criminals committing a digital crime.

The local enforcement officers should preferably be fully equipped with the necessary knowledge of both technology and the legal framework of such complaints. In Malaysia, local police have established a unit to address cybercrimes, but these police personnel are not given sufficient exposure and training in the investigation of new types of cyberbullying. Establishing a special task force for cyberbullying may also demand more time, resources, and skills. The reason is the fear of the nature and appearance of cyberbullying conduct, where it can conceal and act discreetly without ever being traced. The arrest may be difficult to make due to the limited technologies also held by these enforcers. Moreover, as technology evolves, cyberbullying becomes very difficult to track. Once the information is posted on the internet, it may be forever available and may appear anywhere in the world with a potentially vast audience. Customers or victims must overlay their information within the framework of the Communication and Multimedia Act or underlying regulations to provide a more complete picture to the Commission before any action can be taken. A well-educated public awareness campaign on the problem of cyberbullying may therefore also benefit the enforcers.

Proposed Changes in Legislation

The current challenges in prosecuting cyberbullying make reforms necessary. For example, the Penal Code must be amended to prohibit cyberbullying in Malaysia in order to plug existing loopholes. The amendments must include a section on cyberbullying, and the existing sections related to offences, such as criminal defamation, intimidation, and harassment, should also be amended to include threats made by way of electronic communication. Further, the penalty for cyberbullying under the proposed act of stealing personal information must be amended in order to increase the fine and prison term to serve as a greater deterrent. At the same time, the new law should empower courts to impose orders or injunctions to provide for the protection and safety of victims of cyberbullying. Moreover, the legislation should include enhanced protective measures, such as restraining or cyber safety orders, to protect the well-being and life of a victim.

Also, if there are increasingly greater possibilities for potential criminals to use more sophisticated technology, the law should include flexibility that would accommodate some advancements in technology. To gather broad views on certain areas—such as the experiences and knowledge of the stakeholders, it is recommended that a call for feedback be issued. This will help create a comprehensive legal landscape. Finally, to better meet the needs of victims while addressing concerns about trivializing criminal liability and the efficiency and proportionality of criminal responses, it is proposed that the list of specific constituent elements

of the cyberbullying offence should be clarified. Such a proposal would create a proactive legal framework to filter out complex or hard-to-crack cyberbullying cases.

Conclusion

In light of the pervasive and detrimental effects of cyberbullying, the need for clear, precise, and enforceable legislation in Malaysia is paramount. The proposed changes in legislation serve as a crucial step toward addressing online harassment by establishing a comprehensive legal framework that ensures accountability, victim protection, and effective enforcement mechanisms. A well-drafted law, underpinned by unambiguous language and robust implementation strategies, will not only enhance legal clarity but also foster greater public awareness and compliance. Moving forward, a multi-stakeholder approach involving policymakers, law enforcement agencies, digital platforms, and civil society is essential to strengthen regulatory measures and promote a safer online environment. By adopting a proactive and evidence-based legal response, Malaysia can mitigate the harms of cyberbullying and uphold the fundamental rights and well-being of its citizens in the digital age.

Acknowledgements

The authors would like to express their heartfelt appreciation to Global Academic Excellence (M) Sdn Bhd for their invaluable support and for accepting this article for publication, and the Kedah State Research Committee, UiTM Kedah Branch, for the generous funding provided under the Tabung Penyelidikan Am. This support was crucial in facilitating the research and ensuring the successful publication of this article.

References

- Abd Aziz, A., Mohd Noor, N. A., Mohamad, A., Md Isa, Y., Ibrahim, H., Ghazali, O., & Zulkifli, A. (2022). Cyberbullying: Analysis of laws in Malaysia. *International Journal of Law, Government and Communication*, 7, 276–284. <https://doi.org/10.35631/IJLGC.729019>
- Ahmad Razali, N. H. B., Ismail @Nawang, N. B., Syed Nong Mohamad, S. N. A. B., Abdul Ghani, F. B., & Mohd Rasli, M. A. B. (2020). Child cyber bullying: An overview of the legal protection in Malaysia. In N. S. Othman, A. H. B. Jaaffar, N. H. B. Harun, S. B. Buniamin, N. E. A. B. Mohamad, I. B. M. Ali, N. H. B. A. Razali, & S. L. B. M. Hashim (Eds.), *Driving sustainability through business-technology synergy* (Vol. 100, pp. 895-900). European Publisher. <https://doi.org/10.15405/epsbs.2020.12.05.98>.
- Ahmad Razali, N., Ismail Nawang, N., & Mohamad, S. (2022). Cyberbullying in Malaysia: An analysis of the existing laws. *International Journal of Law, Government and Communication*, 7(3), 124–135. <https://doi.org/10.35631/IJLGC.730011>
- Ardiyani, I., & Muhdi, N. (2021). Cyberbullying and suicidal behavior. *International Journal of Research Publications*, 92, <https://doi.org/10.47119/IJRP100921120222653>
- Barlett, C. P., DeWitt, C., Maronna, B., & Johnson, K. (2018). Social media use as a tool to facilitate or reduce cyberbullying perpetration: A review focusing on anonymous and non-anonymous social media platforms. *Violence and Gender*, 5(2), xx-xx. <https://doi.org/10.1089/vio.2017.0057>
- Benito, Á., et al. (2021). Changes that should remain in higher education post-COVID-19: A mixed-methods analysis of the experiences at three universities. *Higher Learning*
- Channel News Asia. (2024, January 10). Malaysia's Esha Rajeshwary Appahu: Cyberbullying victim's tragic story sparks calls for legal reform. *Channel News Asia*. <https://www.channelnewsasia.com>

- DePaula, N., Fietkiewicz, K. J., Froehlich, T. J., Million, A. J., Dorsch, I., & Ilhan, A. (2018). Challenges for social media: Misinformation, free speech, civic engagement, and data regulations. *Proceedings of the Association for Information Science and Technology*, 55(1), 665–668
- De Paoli, S., Johnstone, J., Coull, N., Ferguson, I., Sinclair, G., Tomkins, P., ... & Martin, R. (2021). A qualitative exploratory study of the knowledge, forensic, and legal challenges from the perspective of police cybercrime specialists. *Policing: A Journal of Policy and Practice*, 15(2), 1429-1445. abertay.ac.uk
- El Asam, A., & Samara, M. (2016). Cyberbullying and the law: A review of psychological and legal challenges. *Computers in Human Behavior*, 65, 127–141. <https://doi.org/10.1016/j.chb.2016.08.012>
- Falla, D., Romera, E. M., & Ortega-Ruiz, R. (2021). Aggression, moral disengagement, and empathy: A longitudinal study within the interpersonal dynamics of bullying. *Frontiers in Psychology*. <https://www.frontiersin.org>
- Fernanda, A., & Carla, E. (2023). Differential impact of cyberbullying and verbal bullying on depression levels in late adolescence. *Acta Psychologica*. <https://www.pelnus.ac.id>
- Gong, Y., Gao, X., Li, M., & Lai, C. (n.d.). Cultural adaptation challenges and strategies during study abroad: New Zealand students in China. *Language*. <https://www.um.edu.mo>
- Hoekman, B., & Mavroidis, P. C. (2021). WTO reform: Back to the past to build for the future. *Global Policy*. <https://www.wiley.com>
- Islam, K. N., Sobur, A., & Kabir, M. H. (2023). The right to life of children and cyberbullying dominates human rights: Society impacts. *SSRN Electronic Journal*. <https://www.ssrn.com>
- Ismail, S. M., Teoh, S. Y., & Hussein, S. M. (2022). Taking and sharing photographs of virtual court proceedings to social media: A critical appraisal on the law of contempt in Malaysia. *International Journal for Court Administration*, 13(2). <https://www.iacajournal.org>
- Jayabalan, P., Ibrahim, R., & Manaf, A. (2014). Understanding cybercrime in Malaysia: An overview. *SHS Web of Conferences*, 2(2). <https://doi.org/10.11113/SH.V2N2.424>
- Krešić Ćorić, M., & Kaštelan, A. (2020). Bullying through the Internet – Cyberbullying. *Psychiatria Danubina*, 32(Suppl 2), 269–272.
- Mahmood, A., Hashim, H. N., Zain, F. M., Suhaimi, N. S., & Yahya, N. A. (2018). A survey on the culture of online shaming: A Malaysian experience. *International Journal of Academic Research in Business and Social Sciences*, 8(4), 111-123.
- Martin, D. E., et al. (2025). Prevention of trafficking in organs, tissues, and cells. *Transplantation*, 109(1), 88-97. <https://www.researchgate.net>
- Mawardah, C., et al. (2018). The factors of cyberbullying and the effects on cyber victims. *International Journal of Academic Research in Business and Social Sciences*, 2454-6186.
- McKoy, C. (2021). Law Enforcement Officers' Perceptions in Combating Cybercrime at the Local Level. waldenu.edu
- Mohamad, Z., Ismail, Z., & Thani, A. (2023). Determinants of fraud victimizations in Malaysian e-commerce: A conceptual paper. *International Journal of Academic Research in Business and Social Sciences*, 13. <https://doi.org/10.6007/IJARBSS/v13-i12/20395>
- Noor, N., & Abdul Hamid, B. (2021). Cyberbullying in the name of God: Critical discourse analysis of online responses to the act of de-hijabbing in Malaysia. *3L: Southeast Asian Journal of English Language Studies*, 27(4). <https://www.researchgate.net>

- Olweus, D. (1994). Bullying at school: Basic facts and effects of a school-based intervention program. *Journal of Child Psychology and Psychiatry*, 35(7), 1171–1190.
- Parkins, I. S., Fishbein, H. D., & Ritchey, P. N. (2006). The influence of personality on workplace bullying and discrimination. *Journal of Applied Social Psychology*, 36(10), 2554-2577.
- Patchin, J. W., & Hinduja, S. (2011). Traditional and nontraditional bullying among youth: A test of general strain theory. *Youth & Society*, 43(2), 727–751
- Qazi, K.A., & Hamid, S. (2023). Cyberthreats, cyberbullying, and cyberstalking: a critical examination of digital harassment in the contemporary era. *ShodhKosh: Journal of Visual and Performing Arts*, 4(1), Article 3132. <https://doi.org/10.29121/shodhkosh.v4.i1.2023.3132>
- Rasli, M. R., Manaf, H. B., & Ismail, M. B. (2018). Lessons from Malaysian local government: Does resource management matter in enforcement actions? *The Journal of Social Sciences Research. Research Communications*, 11, 4. <https://www.waldenu.edu>
- Reuters. (2024, July 24). *Malaysia seeking social media platforms' commitment to tackle cybercrimes*. Reuters. <https://www.reuters.com/technology/malaysia-seeking-social-media-platforms-commitment-tackle-cybercrimes-2024-07-24/>
- Scheithauer, H., et al. (2021). Types of cyberbullying. In *The Wiley Blackwell Handbook of Bullying: A Comprehensive and International Review of Research and Intervention* (Vol. 1, pp. 120-138). Wiley.
- Shetgiri, R. (2013). Bullying and victimization among children. *Advances in Pediatrics*, 60(1), 33–51. <https://doi.org/10.1016/j.yapd.2013.04.004>
- Shukor, S. A., & Osman, N. D. (2022). Sexting among children: Differences in law between Malaysian, English, and American laws. *Asian Journal of Applied Communication (AJAC)*, 2022, 31-45. <https://www.researchgate.net>
- Sipalan, J. (2023, December 27). Malaysia to criminalise cyberbullying after influencer suicide. *South China Morning Post*. <https://www.scmp.com/week-asia/politics/article/3270630/malaysia-criminalise-cyberbullying-after-influencer-suicide>
- Suhana, I., et al. (2021). Prevalence of cyberbullying victims and its associated factors among Form 2 and Form 4 secondary school students in Kuala Terengganu, Malaysia. *Asian Journal of Medicine and Biomedicine*, 5(1), 33-40. <https://doi.org/10.37231/ajmb.2021.5.1.412>
- Verma, K., et al. (2023). Leveraging machine translation for cross-lingual fine-grained cyberbullying classification amongst pre-adolescents. *Natural Language Engineering*, 29(6), 1458-1480. <https://www.cambridge.org>
- Westmoreland, K., & Kent, G. (2015). *International law enforcement access to user data: A survival guide and call for action*. SSRN. <https://doi.org/10.2139/ssrn.2547289>
- Wilson, T. J. (2020). Collaborative justice and harm reduction in cyberspace: Policing indecent child images. *The Journal of Criminal Law*, 84(5), 474-496. <https://doi.org/10.1177/0022018320952560>
- Windisch, S., et al. (2022). Online interventions for reducing hate speech and cyberhate: A systematic review. *Campbell Systematic Reviews*, 18(2), e1243. <https://www.wiley.com>
- Xu, Y., & Trzaskawka, P. (2021). Towards descriptive adequacy of cyberbullying: Interdisciplinary studies on features, cases, and legislative concerns of cyberbullying. *International Journal for the Semiotics of Law - Revue Internationale de Sémiotique Juridique*, 34(4), 929-943. <https://www.springer.com>

Yu, M., & Riddle, K. (2022). An experimental test of the effects of digital content permanency on perceived anonymity and indirect effects on cyberbullying intentions. *Social Media + Society*, 8(1). <https://doi.org/10.1177/20563051221087255>