



MEDIA MATTERS VOL. 4

(ADVANCE COPY)

DIGITAL SOCIETY RESEARCH REPORT



[This is an advance copy of the Digital Society Research Grant research summary findings for the 2020 cohort of grant recipients in order to facilitate dissemination and circulation of these research works.]

The Advance Copy is available for a limited duration ahead of the final version].

MALAYSIAN COMMUNICATIONS AND MULTIMEDIA COMMISSION, 2021

The information or material in this publication is protected under copyright and, save where otherwise stated, may be reproduced for non-commercial use provided it is reproduced accurately and not used in a misleading context. Where any material is reproduced, the Malaysian Communications and Multimedia Commission (MCMC), as the source of the material, must be identified and the copyright status acknowledged.

The permission to reproduce does not extend to any information or material the copyright of which belongs to any other person, organisation or third party. Authorisation or permission to reproduce such information or material must be obtained from the copyright holders concerned. This work is based on sources believed to be reliable, but the Malaysian Communications and Multimedia Commission does not warrant the accuracy and completeness of any information and cannot accept responsibility for any error or omission.

Published by:

Malaysian Communications and Multimedia Commission

MCMC Tower 1, Jalan IMPACT
63000 Cyberjaya, Selangor
Tel: +603 8688 8000
<https://www.mcmc.gov.my>

CONTENTS

i	Do Mobile Apps Help to Grow Your Business? The Case of Delivery Services in Sabah - Universiti Malaysia Sabah	3
ii	Factors Affecting Consumers' Cashless Payment Behaviours Amidst the Covid-19 Pandemic - Universiti Utara Malaysia	13
iii	Efficient Web Disclosure Practices Among Malaysian Non-Profit Organisations - Universiti Teknologi MARA	27
iv	IT Skills Among Marginalised Community: The Case of Orphans and Vulnerable Children (OVC) in Malaysia - Universiti Putra Malaysia	40
v	Can Smart Phones Support the Homeless during the Covid-19 Pandemic: A Case Study in Malaysia - Universiti Utara Malaysia	44
vi	B40 Income Earners' Digital Literacy: A Focus on Children at Projek Perumahan Rakyat (PPR) - International Islamic University Malaysia	53
vii	Too Young Too Digital: How Malaysian Parents Mediate Their Young Children's Internet and Digital Device Use - International Islamic University Malaysia	67
viii	Using Survival Data Analysis Perspective to Manage Movement Control Order in Selected Countries: Lessons for Malaysia - University Nottingham Malaysia	81
ix	Malaysian Cyberbullying Law: A Work-in-Progress - Universiti Utara Malaysia	92
	CONTACT US	106

Malaysian Cyberbullying Law: A Work-in-Progress

ANI MUNIRAH MOHAMAD, AHMAD SHAMSUL ABD AZIZ, NOR AZLINA MOHD NOOR,
YUSRAMIZZA MD ISA @ YUSUFF, HUDA HAJI IBRAHIM & OSMAN GHAZALI

Universiti Utara Malaysia

ABSTRACT

In Malaysia, cyberbullying cases are on the rise without any specific legal sanctions to manage them. Cyberbullying should be addressed so that its most harmful consequences such as suicide, theft, and rape can be prevented. Despite the grievous ramifications, existing laws are inadequate to manage cyberbullying matters. Hence, this research aims to break new ground in the existing literature by analysing the adequacy of Malaysian law in addressing cyberbullying as well as considering other jurisdictions' experiences through the adoption of comparative analysis. This research investigated the relevant crucial aspects of existing and potential modalities to deal with cyberbullying that are frequently overlooked. By employing both qualitative and quantitative research methodologies, data was collected using library-based research, field work and online survey. Interviews were conducted with 19 cyberlaw experts and practitioners while an online survey was administered in which 120 respondents from the general public participated. The research findings have indicated that there is no specific law to manage cyberbullying in Malaysia. As it stands, there are laws that potentially cover cyberbullying, albeit not specifically referring to cyberbullying. In the international context, it has been evident from findings of the present study that the international instruments are generally not binding upon Malaysia. The study therefore proposes the creation of a stand-alone law to manage traditional bullying and cyberbullying. Additionally, the study also recommends alternative governing modalities for dealing with cyberbullying at different stages.

Keywords: Bullying, cyberbullying, cybersecurity, cyberlaws

INTRODUCTION

Cyberbullying has become a concern that has translated into law to a larger extent and more technologically mature jurisdictions such as the United States, the United Kingdom, Canada, Australia, and Japan as well as in smaller countries like Singapore and the Philippines. Cyberbullying is analogous to traditional forms of bullying in that it incorporates persistent behaviours that instil apprehension and fear. However, with the advent of new technologies, traditional bullying has taken on entirely new forms through social media mediums such as Facebook and WhatsApp. Thus, it requires explication of new forms of cyberbullying. Cyberbullying takes place when people use, inter-alia, communications technologies, devices, media and platforms in order to harm others.

Problem Statement

A number of problems confront the cyberbullying phenomenon in Malaysia. On the basis of the report issued by the United Nations Children's Fund (UNICEF) in 2019 on violence against children in 30 countries, 3 in 10 young people in Malaysia are victims of cyberbullying (UNICEF, 2019). A total of 28% of the 6,953 young people in Malaysia were recently confirmed being the victims of online abuse, with 43% of them experiencing online private messaging, and gambling through social media apps, including Whatsapp, Facebook, Instagram, Twitter and YouTube. The worrying situation of cyberbullying in Malaysia is further confirmed by empirical data from local research regarding cyberbullying prevalence and incidents (Sivabalan et. al, 2020; Ghazali et. al, 2020; Research Institute Malaysian Youth Development, 2017).

The present laws are inadequate to address cyberbullying matters. The lack of legal attention to the issue of cyberbullying is still a problem facing society today. Analysis of existing cyber laws and traditional criminal laws on cyberbullying has yielded no definite results, which in essence means that at present, cyberbullying by itself, despite its grievous ramifications, is not outlawed in Malaysia. Numerous international and domestic investigations have indicated the association between

cyberbullying and various adverse consequences to the victims such as low self-esteem, anxiety, depression and feeling isolation (Gordon, 2020; Johanis et. al, 2020; Balakrishnan, 2018).

Research Objectives

Therefore, this study aimed at achieving four main objectives:

- 1) To investigate the adequacy of Malaysian laws in addressing cyberbullying;
- 2) To conduct comparative studies of legislation of other countries and highlight areas that local legislation is complementary to and in harmony with international laws, treaties and conventions;
- 3) To identify the gap areas in current laws that need to be developed or enhanced. Additionally, if there were to be specific laws on cyberbullying, to identify which jurisdiction(s) should it fall under; and
- 4) To propose other governing modalities to manage cyberbullying in Malaysia.

LITERATURE REVIEW

Conceptualising Bullying and Cyberbullying

Bullying is the repeated harassment of an individual towards another person through physical violence, name-calling, exclusion, creating false accusations, or any other form of actions that may cause harm (Olweus, 1993). Generally, bullying can be seen as forceful, targeted, calculated, undesirable, immoral, unethical, unaccepted, obscene and offensive actions directed at other people and displaying an imbalance in power (OnlineSense, 2016), which can be true or imagined. These are hardly one-off experiences but they are frequent and periodic. Bullying usually comes in the form of physical attack and verbal assaults which include rumour-mongering, defaming comments, and threats.

The advancement of technology and the Internet has made bullying more difficult to combat and victims easier to be attacked because now, cyberbullies can hide their identity while causing harm to the victim. This anonymity is the most significant difference between traditional and cyberbullying, and it is the Internet that gives such an advantage to the bully. People who suffer from cyberbullying find it almost impossible to track down their oppressors which makes cyberbullies different from the traditional bullies known to everyone.

To further aggravate the situation, cyberbullying is not limited by location, which means that it goes beyond the classroom, school, campus, or neighbourhood to the extreme reaches of the world. A cyberbully who is armed with a laptop, smartphone, or any form of internet access can victimise someone irrespective of the location. Cyberbullying also transcends the limit of time as it can be done speedily, at any time of the day, week, or year. Finally, another significant difference is that cyberbullying is not limited to any specific age group, and the victim might never grow out of it.

In the context of the present study, cyberbullying can therefore have the following operational definitions:

“premeditated, destructive actions, meted out frequently by a person or group of people with the aid of current technologies against an individual less able to fend off such attacks” (Juvonen & Gross, 2008).

“a person or group of people who intentionally use information and communication technologies to promote planned and continuous harassment targeted at another person or group of people by writing or posting vicious messages or using pictures to harm such person” (Mason, 2008).

“a hostile, premeditated action, meted out by a person or group, done repeatedly through the internet to someone who cannot protect him/herself against such attacks” (Smith et al., 2008).

Within the international context, UNICEF has defined “bullying” as “...intentional and aggressive behaviour occurring repeatedly against a victim where there is a real or perceived power imbalance, and where the victim feels vulnerable and powerless to defend himself or herself.” Therefore, when bullying occurs in the online world—through computers, cell phones or other electronic devices—it is referred to it as online bullying or cyberbullying.

Meanwhile, various nations which have their own set of laws on cyberbullying also provide the definition of bullying and cyberbullying. For example, the following excerpt is taken from The Philippines' Anti-Bullying Act of 2013:

Section 2. Acts of bullying - For purposes of this Act, "bullying" shall refer to any severe or repeated use by one or more students of a written, verbal or electronic expression, or a physical act or gesture, or any combination thereof, directed at another student that has the effect of actually causing or placing the latter in reasonable fear of physical or emotional harm or damage to his property; creating a hostile environment at school for the other student; infringing on the rights of the other student at school; or materially and substantially disrupting the education process or the orderly operation of a school.

Generally, these definitions suggest that cyberbullying is the act of bullying taking place in the cyber or virtual world. While both cyberbullying and traditional bullying have similarities such as acts of harassment, threatening and aggression, the cyber environment extends the bullying to provide anonymity, larger time and space that bullying can happen anytime and anywhere. In addition, the bullying act will be permanently stored in cyberspace. This extends the effect of cyberbullying beyond traditional bullying. Thus, cyberbullying in this study has been defined as any bullying such as intimidating, harassment, frightening and threatening through an electronic medium, particularly in cyberspace. Key elements to describe cyberbullying will be proposed from this study.

Existing Cyberbullying Prevention Strategies in Selected Countries

In Malaysia, there are no specific laws for cyber harassment and cyberbullying. Nevertheless, there is a general cyberbullying law which is under the Communications and Multimedia Act 1998. Despite that, it currently does not address specific groups such as students and others. However, the Communication and Multimedia Act 1998 can be used for anything related to cyberbullying such as malicious comments, or which annoying, or insulting that is potentially an offence. On the other hand, the Penal Code could potentially be used for any offline and online physical abuse or death threats if they have been reported. Despite the absence of a specific law in Malaysia, the following efforts have been made to combat cyberbullying, such as Klik Dengan Bijak (KDB) - <http://www.klikdenganbijak.my>, CyberSAFE Malaysia - <https://www.cybersafe.my> as well as CyberSafe in school - <https://cybersafeinschools.my>.

Meanwhile, in the international context, such as in the United States, a customised curriculum called I-SAFE curriculum has been developed covering aspects such as Internet safety, cyber community citizenship, cybersecurity, personal safety, intellectual property, and law enforcement online (Chibnall, Wallace, & Leicht, 2006). Additionally, the community is encouraged to push for anti-bullying legislation and Internet safety policies at the state, local, and district levels (Feinberg & Robey, 2008). Meanwhile, in England, the Department of Education has published a blueprint to deal with cyberbullying at the school level. Comprehensive resources which includes, among others, an interactive anti-bullying information tool for parents and carers and free online training.

In the Philippines, the government has acknowledged cyberbullying as a threat, especially towards children and started to adopt some policies and legal instruments. The Republic Act No. 10627 or the Anti-Bullying Act of 2013 has been enacted to curb cyberbullying among students by making elementary (i.e., primary) and secondary schools prepare and implement guidelines over the matter. On the other hand, in Japan, the Anti-Bullying Act was first initiated by the Japanese government on 28 June 2013, which was then legislated three months later, following the bullying incident of a school student that ended up in suicide. The Act is the first law in Japan that explicitly prevents school bullying. It also includes other related features such as measures for cyberbullying.

The Need for a Specific Legal Framework for Managing Cyberbullying

According to the findings of a global survey, Malaysia is among the world's top countries (i.e., ranked sixth among 28 countries in a study on cyberbullying) where parents have reported their children experiencing cyberbullying (The Star, 2019). The survey found that 23% of Malaysian parents admitted their children had experienced cyberbullying. Another survey by UNICEF revealed a startling 8 out of 10 participants surveyed claimed they had fallen victim to bullying in school (The Star, 2019). Even though cyberbullying incidents are on the rise, Malaysia does not have a specific law pertaining to

cyberbullying. To date, the Philippines and Singapore are the only two Asian countries which have specific laws for cyberbullying, namely, the Protection from Harassment Act (POHA) in Singapore, and the Anti-Bullying Act of 2013 in the Philippines. Although Malaysia has several written rules which can be used to address cyberbullying, the country should have a specific stand-alone law to address the increasing number of cyberbullying cases.

METHODOLOGY

The study employed a phenomenological design in which a key phenomenon is investigated (i.e., cyberbullying). The key elements that were investigated in the study are four-fold in tandem with the objectives of the study, namely, (1) the adequacy of the current Malaysian laws in addressing cyberbullying, (2) the legal position of cyberbullying in the international context (international, regional and other nations), (3) the gaps that exist in the Malaysian laws and the international laws in addressing cyberbullying, and (4) other governing modalities in managing cyberbullying.

In the present study, data was collected using two instruments: firstly, qualitative interviews with experts on cyberlaw from government and non-government organisations, industry practitioners, health practitioners, enforcement officers and higher learning institutions (sample size: 19), and secondly, a quantitative online survey administered to the general public (sample size: 120). The purpose of using two sets of instruments is to enable triangulation to be made between the views of the experts and practitioners with the understanding and perceptions of the general public. This in turn would increase the validity and reliability of the findings of the study. The analysis of qualitative data from the interviews and open-ended question of the survey was carried out using computer-aided qualitative data analysis software ATLAS.ti version 9. The coding process of the data was done using a purely inductive approach, for which the true meanings of the responses from the interview participants and survey respondents were coded into specific themes for the purpose of reporting. Meanwhile, the analysis of the quantitative data from the survey was performed using and retrieved directly from the MS Office Form, for the purpose of reporting.

FINDINGS AND ANALYSIS

Objective 1: Malaysian Laws on Cyberbullying

Malaysia does not have a specific law on bullying, let alone cyberbullying. However, there are laws in Malaysia that are, even though scattered, could potentially cover cyberbullying. Such laws are categorised into general constitutional provisions on freedom of speech, criminal, cyber and civil laws. For this purpose, the following laws could potentially cover cyberbullying within the ambit of this present study:

- a) General provision on freedom of speech
 - Article 10 of Federal Constitution
- b) Criminal law
 - Section 503 and 509 of Penal Code
 - Section 4 of Sexual Offences against Children Act 2017
- c) Cyber law
 - Section 233 of Communications and Multimedia Act 1998
 - Section 36 A and 36B of Copyright Act 1987
 - Section 4 of Computer Crimes Act 1997
- d) Civil law
 - Section 81B of Employment Act 1955
 - Section 20 of Industrial Relation Act 1967
 - Section 15 of Occupational Safety and Health Act 1994
 - Section 4 of Defamation Act 1957
 - Section 130 of Education Act 1996

Nevertheless, these laws have been found to be inadequate to appropriately address cyberbullying in Malaysia. This is understandable given that such laws would be specific for the

purpose in which they have been legislated within the context of their statutes, and no specific reference has been made to bullying or cyberbullying.

Additionally, the data from the interviews indicates that the interview participants observed that cyberbullying should be criminalised, but it might be different for cases involving child perpetrators. In this regard, it was further observed that extended research would need to be carried out to clearly define cyberbullying before it could be treated as a crime. Accordingly, few participants viewed that different forms of punishment should be applied based on the different types or age of perpetrators. In terms of the adequacy of Malaysian laws in addressing cyberbullying, majority of the participants opined that the existing laws had been inadequate and insufficient to properly address cyberbullying.

Objective 2: International Laws on Cyberbullying

Within the context of international laws on cyberbullying, there are various laws which rightly cover cyberbullying expressly or within its context. For this purpose, the following international and regional instruments have been found to be addressing cyberbullying:

- a) Legally binding international instruments
 - Article 19.1 of United Nations Convention on the Rights of the Child (UNCRC)
 - Articles 4 and 5 of Budapest Convention on Cybercrime and Its Additional Protocol
 - The Commonwealth of Independent States' Agreement on Cooperation in Combating Offences related to Computer Information of 2001
 - Arab League's (formerly known as the League of Arab States) Arab Convention on Combating Information Technology Offences of 2010
 - Shanghai Cooperation Organization's Agreement on Cooperation in the Field of International Information Security of 2009
 - African Union Convention on Cyber Security and Personal Data Protection of 2014
 - African Union Convention on the Establishment of a Legal Framework Conducive to Cybersecurity in Africa (2012)
 - Council of European Union's Resolution on a Concerted Work Strategy and Practical Measures Against Cybercrime
 - Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
 - Frame Decision 2005/222/WSiSW [Council Framework Decision 2005/222/JHA of 24 February 2005 on Attacks Against Information Systems]
- b) Non-binding international instruments
 - United Nations Human Rights Council's Resolution on the "Promotion, Protection and Enjoyment of Human Rights on the Internet" [27 June 2016, U.N. Doc. No. A/HRC/32/L.20]
 - United Nations General Assembly's Resolution on the "Right to Privacy in the Digital Age" [Third Committee, 1 November 2013, U.N. Doc. A/C.3/68/L.45]
 - United Nations General Assembly's Resolution on the "Protecting Children from Bullying" [18 December 2014, U.N. Doc. No.A/69/158]
 - United Nations General Assembly's Resolution on the "Protecting Children from Bullying" [19 December 2016, U.N. Doc. No.A/71/176]
 - United Nations General Assembly's Resolution on the "Protecting Children from Bullying" [17 December 2018, U.N. Doc. No.A/73/154]
 - Economic and Social Council's Resolution 2011/33 on Prevention, Protection and International Cooperation against the Use of New Information Technologies to Abuse and/or Exploit Children
 - International Telecommunication Union (ITU) Guidelines on Child Online Protection 2020
 - League of Arab States Model Law on Combating Information Technology Offences (2004)
 - International Telecommunication Union (ITU)/Caribbean Community (CARICOM)/Caribbean Telecommunications Union (CTU) Model Legislative Texts on Cybercrime, e-Crime and Electronic Evidence (2010)
 - Common Market for Eastern and Southern Africa (COMESA) Cybersecurity Draft Model Bill (2011)

What could be gathered from the review of the laws is that international and regional instruments are generally not binding on Malaysia, and even if they were, these international and regional instruments would not provide adequate recourse for cyberbullying.

Additionally, various countries in Asia particularly and around the world have passed their own national laws to specifically manage cyberbullying and harassment. Examples of other nations' laws on cyberbullying are presented below:

- a) Singapore
 - Protection from Harassment Act 2014
 - Computer Misuse and Cybersecurity Act 1993
- b) Japan
 - Act for the Promotion of Measures to Prevent Bullying (2013)
- c) The Philippines
 - Anti-Bullying Act of 2013
 - Revised Penal Code and Cybercrime Prevention Act of 2012
 - Civil Code of the Philippines
 - Labour Code of the Philippines
- h) New Zealand
 - Harmful Digital Communications Act 2015
 - Harassment Act 1997
- i) South Africa
 - Protection from Harassment Act, 2010
- j) United Kingdom
 - Protection from Harassment Act 1997
 - Computer Misuse Act 1990
 - Malicious Communications Act 1988
 - Criminal Justice and Licensing (Scotland) Act 2010
- l) United States (Selected States)
 - Texas' Senate Bill 179 David's Law (2017)
 - California's AB1542, "Jordan's Law" (2017), AB 9 "Seth's Law" (2011) and California Assembly Bill 2291
 - Washington's Rev. Code Wash. (ARCW) § 28A.300.285 (2013)

These selected jurisdictions possess stand-alone legislation to deal with the issue of bullying, cyber bullying and harassment. Generally, these laws provide for legal recognition of bullying, cyberbullying and harassment as a wrong. Not only do these laws provide for the relevant sanctions to the perpetrators of bullying, they also provide for legal remedies and relief to the victims of bullying, as well as prevention strategies to be adopted by the relevant parties such as development of anti-bullying policies in schools and learning institutions (e.g., the Philippines, Singapore, and United Kingdom). Apart from that, a few states have even passed laws for the promotion of good practices of ICT and the Internet as well as prevention of harmful communications (e.g., Australia, Canada, United Kingdom, and New Zealand). Accordingly, other nation's cyberbullying laws (e.g., the Philippines, Singapore, South Korea, Australia, United Kingdom, and New Zealand) are worthy of investigation for lessons learned, to suit local circumstances.

Objective 3: Gaps in Malaysian Laws and International Laws on Cyberbullying

There is an urgent need to address the gaps in the law by the conceptualisation of the general definition of bullying and cyberbullying, determination of duty of care in cyberbullying cases, specification for punishment for perpetrators of cyberbullying, provision of remedies for perpetrators and victims of cyberbullying, and creation of stand-alone legislation to curb cyberbullying. This was concluded after reviewing Malaysian laws as well as international laws on cyberbullying, and considering various aspects as follows:

- a) the non-criminality status of traditional bullying and cyberbullying in Malaysia;
- b) the absence of specific law to address cyberbullying in Malaysia;
- c) the inadequacy of the various laws in Malaysia to address cyberbullying;
- d) the non-applicability of international instruments to the Malaysian context;

- e) the inadequacy of the applicability of cases of international instruments to the Malaysian context to manage cyberbullying in Malaysia;

(1) *Conceptualisation of Legislative Definitions of Bullying and Cyberbullying*

There has been no definite conceptualisation of bullying and cyberbullying under Malaysian law to date; hence, there would be a dire need for the proper conceptualisation of legislative definitions of bullying and cyberbullying in Malaysia, to define what elements and actions constitute bullying.

(2) *Determination of Duty of Care in Cyberbullying Cases*

It would also be pertinent to determine the duty of care in cyberbullying cases, who should be the caretaker of the actions by the perpetrators, and if would make a difference between adult and child perpetrators of cyberbullying. Additionally, it would also be important to determine the duty of care of persons involved in the cyberbullying framework such as the schools, parents, friends and caretakers.

(3) *Specification for Punishment for Perpetrators of Cyberbullying*

There has been a huge gap in the provision of legal sanctions for the punishment for perpetrators of cyberbullying to date; hence, there would need to be a proper specification for such punishment and given the different nature of adults and children, whether there should be a difference in terms of punishment between adult and child perpetrators.

(4) *Provision of Remedies for Perpetrators and Victims of Cyberbullying*

In the absence of legal provisions on the remedies for cyberbullying, no definite relief may be awarded for both perpetrators and victims of cyberbullying. Therefore, there would be an urgent need for specific provisions to be in place to provide for the specific remedies for both perpetrators and victims of cyberbullying.

(5) *Creation of Stand-Alone Legislation to Curb Cyberbullying*

Given the serious ramifications of cyberbullying, it would be pertinent for steps be taken to draft a specific and stand-alone legislation on anti-bullying and anti-cyberbullying.

Objective 4: Alternative Governing Modalities for Cyberbullying

The data from interviews and survey indicate that there were various potential governing modalities for cyberbullying that could be adopted, apart from creation of specific laws to govern this act. First and foremost, existing efforts by the government and non-governmental organisations were in abundance. The interviewed experts outlined various programmes and efforts in curbing cyberbullying, as illustrated in the following Figure 1.

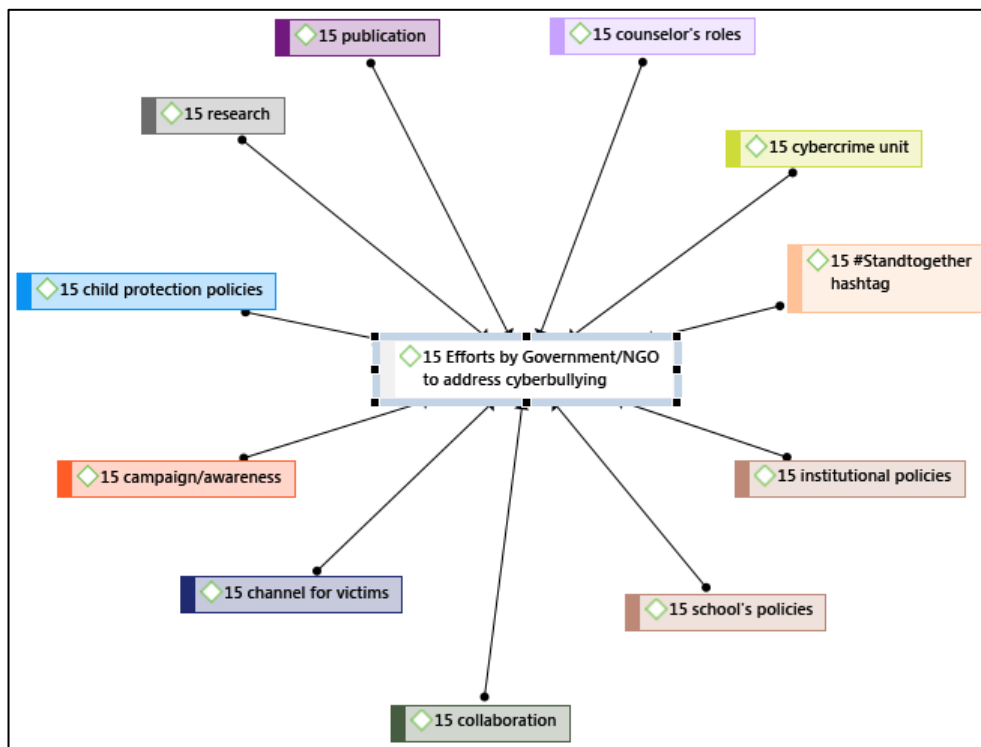


Figure 1: Interview Participants' Views on the Existing Efforts by Organisations in Curbing Cyberbullying

In this regard, such governing modalities as proposed by the interview experts could be divided into two parts, namely, (1) preventive measures, and (2) handling of cyberbullying cases, as illustrated in the following Figure.

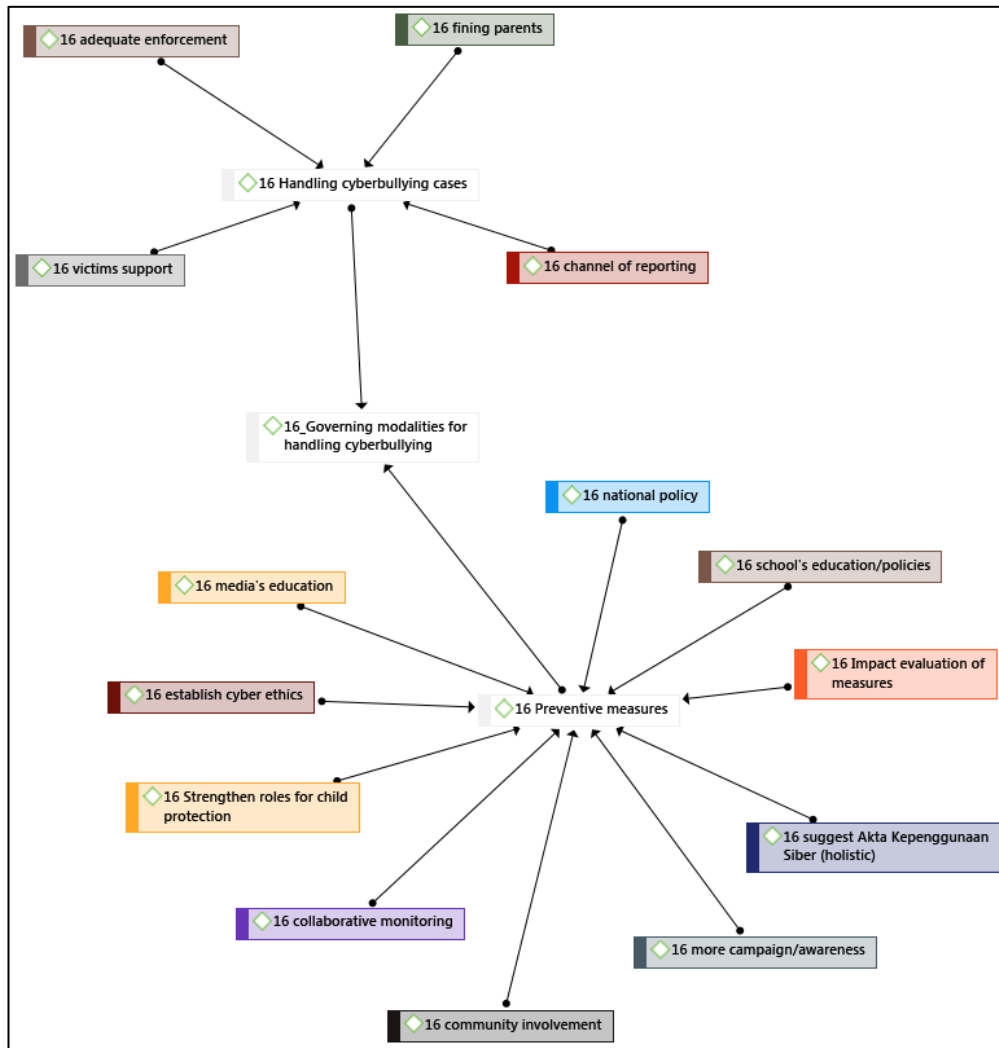


Figure 2: Interview Participants' Views on the Governing Modalities for Cyberbullying

In terms of governing modalities for cyberbullying, the management and control of cyberbullying could be divided into two main dimensions, namely, the preventive measures (i.e., before cyberbullying happens, so as to prevent the potential occurrence of cyberbullying itself), and the handling of cyberbullying cases (i.e., upon occurrence of cyberbullying incidents).

- (1) **Preventive Measures:** Preventive actions should include the establishment of internal policies against bullying and cyberbullying in schools, organisations/ institutions or workplaces. Such policies should be made accessible by the students, parents, workers, members of staff and persons related to the business affairs of the organisation/institution. Apart from that, efforts should also be in place to strengthen the family institutions. This follows the idea that family institutions play a vital role in the shaping and development of an individual's personality. Among others, families should be mindful of their children, so as to take part in their children's lives and engage with their social and daily needs.
- (2) **Handling of Cyberbullying Cases:** When a cyberbullying incident takes place, there should be clear, convenient and quick channels for reporting incidents. Such channels should be made clear to the general public, so as to ensure the proper handling of perpetrators and victims of cyberbullying. Additionally, protection for perpetrators and victims should also be in place, such as rehabilitation programmes, counselling sessions, compensation scheme, and other situations for the handling of cyberbullying perpetrators and victims.

RECOMMENDATION

Based on the key findings of the study, this section will present the recommendations of the study. In completing the study entitled, “The Adequacy of Malaysian Laws in Regulating Cyberbullying”, the researchers hereby offer the following two recommendations to address this issue. First, the researchers recommend the creation of specific law to address bullying, and second, the researchers recommend the establishment of a working committee as the focal point for coordination of bullying and cyberbullying cases.

Recommendation 1: Creation of a Specific Law to Address Bullying

It is hereby proposed that a specific law is created to address bullying in general, and cyberbullying in particular. The proposed name for the law is: “Anti-Bullying Act”. This recommendation comes in light of the passing of similar laws in the Philippines and various states in the United States, as well as the general laws in Singapore, United Kingdom, and New Zealand. Particularly, the action plan consists of three stages:

Stage 1 – Lessons Learned from Other Jurisdictions

Laws on anti-bullying and protection from harassment which had been passed in other nations’ jurisdictions should serve as lessons to be learned, with intended adoption in Malaysia where applicable to suit to local circumstances. Relevant pieces of legislation from Asian countries, such as Philippines’ Anti-Bullying Act 2013 and Singapore’s Protection from Harassment Act, as well as laws from non-Asian countries such as United Kingdom’s Protection for Harassment Act 1997 and New Zealand’s Harmful Digital Communications Act 2015 are hereby recommended to serve as a guide to be adopted in Malaysia.

Stage 2 - Strengthen the Resilience and the Role of the Local Community

The local community’s resilience and role should be enhanced and strengthened for the proper prevention and handling of cyberbullying cases. Therefore, it is hereby recommended that input be requested from the public and private offices, including the non-governmental organisations (NGOs), enforcement officers, family institutions, counsellors, social workers and other relevant parties.

Stage 3 - Drafting of an Anti-Bullying Bill

With appropriate understanding of other nations’ laws on anti-cyberbullying, the Malaysian government is suggested to proceed with drafting of the bill by appointment of legal drafters that would focus on the proposed key features of the “Anti-Bullying Act. Additionally, it is also proposed that the legal drafters should invite public participation/ consultation with the aim of generating holistic views by combining the top-down approach by legislatures and the bottom-up approach from citizens for the betterment of the nation as a whole.

It is hereby proposed that the relevant authority to oversee this “Anti-Bullying Act” is the Royal Malaysia Police or *Polis Diraja Malaysia* (PDRM) given that the proposed key features of the Act consist of both civil and criminal matters, and PDRM has the means, capability and expertise to manage the issues related to bullying and cyberbullying. Produced below are the proposed key features of the “Anti-Bullying Act”.

Table 1: Proposed Key Features of the “Anti-Bullying Act”

Item	Suggested Key Feature
1. Preamble	While outlining the adverse consequences of both traditional and cyberbullying on people, the preamble conveys explicit prohibitions against bullying in Malaysia. It further communicates the purpose and importance of the law.
2. Definition and Elements	It defines bullying behaviour and what types of actions and conditions related to traditional and cyberbullying are prohibited. It clearly demarcates the core elements of prohibited traditional and cyberbullying.
3. Application	The law directly applies to perpetrators and victims of bullying of all ages. It may enumerate specific characteristics to convey

Item	Suggested Key Feature
	legal protections for certain classes of individuals such as children or for any person who is bullied based on individual characteristics including weight, physical appearance, gender identity, ethnicity and socio-economic status.
4. Remedies	The law determines, creates and adopts criminal or civil actions for prohibited offline bullying and online bullying according to their established types and elements. The determination of such actions should also be tailored to suit the adult and child bullies.
5. Preventive Strategies	The law articulates guidelines and expectations relating to specific preventive strategies against traditional bullying and cyberbullying, particularly anti-bullying policies. It sets requirements for workplaces and schools to develop anti-bullying policies. Additionally, the policies need to provide not only a definition of bullying behaviour which is compatible with national law but also the scope of traditional and cyberspace bullying that create a hostile environment at workplaces and schools. The policies should further outline procedures including written documentation of reported incidents of bullying at workplaces and schools.
6. Mechanism for handling bullying cases	The law creates mechanisms for handling bullying cases, encompassing reporting, jurisdiction of the court, enforcement of court orders, counselling for victims/ perpetrators, rehabilitation programmes, protection order and community service. It further delineates prescriptively their specific components and requirements to guide their development and implementation.
7. Punishment for the perpetrators	The law includes specific provisions addressing consequences or punishments for traditional bullying and cyberbullying behaviour. The punishments vary in accordance with the classifications of perpetrators (i.e., adult perpetrators and child perpetrators falling under the purview of convictions).
8. Remedy/Rights for the victims	The text of legislation communicates legal assurances to bullying victims of their rights. The laws explicitly guarantee the avenues of recourse for addressing concerns regarding prohibited bullying, such as compensation scheme, injunction order, medical intervention, expedited order and removal of abusive content. The statements relating to the legal assurances vary with respect to the specificity of victims' rights.

Proposed elements of bullying

Accordingly, by reference to the conceptualisation of bullying in other nations' laws, the following are the elements of bullying to be adopted in the proposed "Anti-Bullying Act":

- Actus Reus – to harass, threat, abuse/insult, cause alarm and distress, provoke, incite hatred, humiliate
- Mens Rea – intention or knowledge
- Impacts on victims – alarming feelings and causing distress, damage to a victim's psyche and/or emotional well-being/undue emotional distress
- Specific subject matters – Actions, acts, statement, behaviour relating to race, colour, religion, sex, disability and national origin (criminal sanction or civil remedy)

Based on the aforementioned key elements, the following examples may be useful to clarify the description of traditional bullying or cyberbullying:

- (1) *A instructs B to complete A's homework. If B disagrees, A threatens to do something bad to B. B experiences physical and emotional distress. A commits bullying.*
 - (2) *A incites hatred towards B, a person of different skin colour. A calls upon other friends to hate B. B experiences damage to his emotional well-being. A commits bullying.*
 - (3) *A, with intention to insult B, transmits insulting private messages to B via social media messaging. As a result, B experiences emotional distress. A commits cyberbullying.*
 - (4) *A, by using a fake social media account, posts humiliating images of B. A has the knowledge that the postings would indeed humiliate B. As a result, B experiences alarming feeling and humiliation. A commits cyberbullying.*
 - (5) *A posts on his social media account a provoking statement relating to a certain religion. A does not have the intention to cause provocation nor the knowledge that such posting is provocative. A does not commit cyberbullying.*
- (To also be introduce in the Literature Review section)*

Proposed application of the Act

Meanwhile, the following applications of the Act are proposed, in which the Act would include provisions for addressing:

- Adult and child victims of bullying: This follows the fact that both adults and children could fall victims of bullying; hence, legal provisions safeguarding their rights and avenues should be in place.
- Adult of child perpetrators of bullying: This is justified given that both adults and children could become perpetrators of bullying. In essence, different treatments should be in place for adults as against child perpetrators of bullying, due to different physiological and nature of adults and children.
- Stakeholders for cyberbullying, such as schools, policy makers, solicitors, social workers, etc: Stakeholders are essential parties in the chain of bullying and cyberbullying matters, particularly given that different stakeholders have their respective expertise and way of handling things. Therefore, it is justified to have the proposed new Bullying Act to contain provisions for rights and duties of stakeholders in matters pertaining to bullying.
- Protected class: Actions, acts, behaviour, statements or caricature that relates to race, colour, religion, sex, disability and national origin. Such actions which relate to certain matters should be clearly set out in the Act.

Recommendation 2: Establishment of Working Committee as Focal Point for Coordination of Bullying and Cyberbullying Cases

The second recommendation by the researchers is for the establishment of a working committee to serve as a focal point for the coordination of bullying and cyberbullying cases. The committee should oversee two important aspects of bullying and cyberbullying, namely, the prevention strategies, and the handling of bullying and cyberbullying incidents.

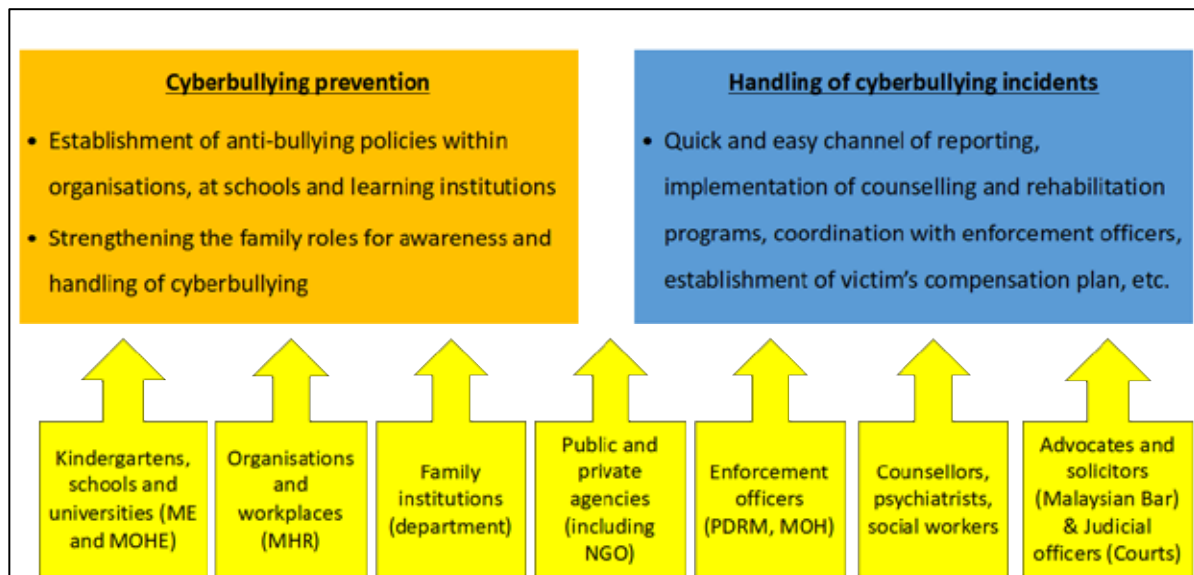


Figure 3: Working Committee as Focal Point for Coordination of Bullying and Cyberbullying Cases

Prevention of Bullying and Cyberbullying

The Committee shall oversee the coordination and establishment of anti-bullying policies within organisations, at schools and learning institutions. Additionally, the committee shall also promote the strengthening of family roles for awareness and handling of bullying and cyberbullying.

Handling of Bullying and Cyberbullying Incidents

The committee shall establish or cause to be established a quick and easy channel for reporting bullying and cyberbullying incidents. Apart from that, it is also pertinent to have appropriate implementation of counselling and rehabilitation programmes for both perpetrators and victims of bullying and cyberbullying cases with the coordination with enforcement officers and relevant parties. The committee should also evaluate the necessity for the establishment of a victim's compensation plan in providing the appropriate remedies for the victims of bullying and cyberbullying cases.

Among the parties to be involved in this committee, either as a member or contact persons, are:

- 1) Kindergartens, schools and universities (Ministry of Education and Ministry of Higher Education);
- 2) Organisations and workplaces (Ministry of Human Resources);
- 3) Family institutions (government and private departments involved);
- 4) Public and private agencies (including NGOs);
- 5) Enforcement officers (including Royal Malaysia Police and Ministry of Health);
- 6) Counsellors, psychiatrists and social workers; and,
- 7) Advocates and solicitors (Malaysian Bar) and judicial officers (the courts).

CONCLUSION

The study investigated the adequacy of Malaysian laws in addressing cyberbullying and studied the legal position of cyberbullying in the international context for comparative analysis. Further, the study identified the gaps in current laws which need improvement and enhancement, as well as proposed alternative governing modalities for the management of bullying and cyberbullying in Malaysia.

Essentially, the current landscape of cyberbullying in Malaysia is that Malaysia does not have a specific law to govern cyberbullying. Although there are some laws that address some aspects of bullying, such laws are inadequate to provide for cyberbullying. For this purpose, a study was carried out involving 19 interview participants and 120 survey respondents. Therefore, it is suggested that there need to be a holistic approach to address issues encompassing (1) protection of victims of bullying (2) sanctions to perpetrators (3) compensatory aspects (4) prevention of bullying, and (5) handling mechanism of bullying cases.

Accordingly, the future of the legal framework governing cyberbullying should be in the form of an integrated and holistic approach with appropriate recognition and highlighting of risk and harms through legislative instruments. Provisions should be made for duty of care and multiple governing modalities to properly address bullying. Similarly, immediate action is recommended towards the development of legislative instruments, identification of relevant agencies/stakeholders and setting of governing modalities for addressing traditional bullying and cyberbullying.

REFERENCES

- Balakrishnan, V. (2018). Actions, emotional reactions and cyberbullying—From the lens of bullies, victims, bully-victims and bystanders among Malaysian young adults. *Telematics and Informatics*, 35(5), 1190-1200.
- Chibnall, S., Wallace, M., & Leicht, C. (2006). Final Report: I-safe evaluation. Retrieved from <http://www.ncjrs.gov/pdffiles1/nij/grants/213715.pdf>
- Chin, C. (2017). Govt Out to Put a Stop to Cyberbullying. *The Star Online*. Retrieved. Retrieved from <https://www.thestar.com.my/news/nation/2017/06/18/govt-out-to-put-a-stop-to-cyberbullying-steps-are-being-taken-to-ensure-our-kids-are-safe-online>
- Feinberg, T., & Robey, N. (2008). Cyber bullying. *Principal Leadership (Middle School Edition)*, 9(1), 10-14.
- Ghazali, A. H. A., Samah, A. A., Omar, S. Z., Abdullah, H., Ahmad, A., & Shaffril, H. A. M. (2020). Predictors of Cyberbullying among Malaysian Youth. *Journal of Cognitive Sciences and Human Development*, 6(1), 67-80.
- Gordon, S. (2020). 8 Motives Behind Why Kids Cyberbully. Retrieved from <https://www.verywellfamily.com/reasons-why-kids-cyberbully-others-460553>
- Johanis, M. A., Bakar, A. R. A., & Ismail, F. (2020, April). Cyber-Bullying Trends Using Social Media Platform: An Analysis through Malaysian Perspectives. In *Journal of Physics: Conference Series* (Vol. 1529, No. 2, p. 022077). IOP Publishing.
- Juvonen, J., & Gross, E. F. (2008). Extending the school grounds? - Bullying experiences in cyberspace. *J. Sch. Health*, 78(9), 496-505. doi:10.1111/j.1746-1561.2008.00335.x
- Mason, K. L. (2008). Cyberbullying: A preliminary assessment for school personnel. *Psychol. Sch.*, 45(4), 323-348. doi:10.1002/pits.2030
- Olweus, D. (1993). *Bullying at school.*, MA: Blackwell. Malden, MA: Blackwell Publishing.
- OnlineSense. (2016, Sep 26, 2016). 5 Differences between Cyber Bullying and Traditional Bullying. Retrieved from <https://onlinesense.org/5-differences-cyber-bullying-traditional-bullying/>
- Research Institute Malaysian Youth Development. (2017). *Buli siber dalam Kalangan Remaja Di Malaysia*. (Kuala Lumpur, Penerbit Kementerian Belia dan Sukan).
- Sivabalan, T. V., Zaki, R. A., & Yuen, C. W. (2020). The prevalence of cyberbullying and its associated factors among young adolescents in penang, malaysia. *Journal of Health and Translational Medicine*, 23(Supplement), 202-211.
- Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., S. Russell, & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry and Allied Disciplines*, 49(4), 376-385. doi:10.1111/j.1469-7610.2007.01846.x
- UNICEF (2019) Cyberbullying and online violence in Malaysia, online available at <https://malaysia.ureport.in/> accessed 28 September 2020.

CONTACT US

For any enquiries, please contact the Digital Society Research Grant secretariat:

Research Enterprise Department
MCMC Academy
Centre of Excellence (CoE)
Malaysian Communications and Multimedia Commission
Jalan IMPACT, 63000 Cyberjaya
Selangor
Tel: +603 8688 7854/8354
Email: dsrg@mcmc.gov.my