International Journal of Advanced Science and Technology
Vol. 29, No. 8, (2020), pp. 143-154

Legal Framework on Protection of Children against Cyberbully in Malaysia: A Cause of Great Concern

Zainal Amin Ayub[1], Zuryati Mohamed Yusoff[2], Md. Zahurul Haq[3]

[1,2,3]*School of Law, Universiti Utara Malaysia*
[1]*z.amin@uum.edu.my*, [2]*zuryati@uum.edu.my*, [3]*md.zahurul@uum.edu.my*

Abstract

While modern information technology has brought revolutionary changes in the way people communicate and socialise in one hand, it has become a sophisticated tool for severe violation of privacy and harassment in the other hand. Cyberbullying has become a great concern over the last few decades with rapid development and availability of modern information technology in many parts of the world including Malaysia. Several incidents of online harassments of young children resulting in tragic consequences raised the question as to how to control this menacing phenomenon in online world. As the development of technology is always faster than the governing laws, researchers and legislators finding it difficult to define and answer the legal issues raised by cyberbullying. Specially, in a country like Malaysia where there is no specific legislation to handle perpetration of cyberbullying, authorities must try to find solution in the existing framework of criminal proceeding and social dialogue to protect the children online.

Keywords: *Cyberbullying, Online, Children, and CyberSecurity.*

1. Introduction

In the current age of technology, the development of the technological communication has created new and sophisticated issues. Whilst most adults are astonished by the speed of the technology is advancing, it is otherwise to the young netizens where it has become the norm (Ayub & Yusoff, 2018, p. 222; Patel, 2012, p. 590). The Internet offers numerous benefits for the young such as developing and updating their knowledge, build up soft skills and an avenue for them to make new friends. Along with the tremendous benefits offered by the Internet, it also hosts the dangers such as cyberbullying, hacking, voyeurism, identity theft, phishing and many other online crimes that have yet to appear (Jalil, 2011, p. 211). Hence, Internet is regarded as a double-edged sword since it has good sides and ugly sides (King, 2010, p. 846). This shows that the children and youngster are not entirely safe in the cyber space despite of the fascinating characteristics of the Internet.

According to Najib, the ex-Prime Minister of Malaysia, online threats against children are categorized into cyber grooming, cyber pornography, cyberbullying and identity theft (Anis, Rahim & Lim, 2012). As reported by the CyberSecurity Malaysia, cyberbullying and identity theft are on a rampage (Hiichiikok Foundation, 2013). As regard to cyberbullying, the sharp increasing of number of cyberbullying incidents is not only faced by Malaysia but also by many other countries. For example, it was reported that the number of cases of cyberbullying in the UK shot up from 2,410 in the year 2011 to 4,507 in 2012-2013 (Sellgren, 2014), and a 2019 study conducted by United Nations International Children's Emergency Fund (UNICEF) indicated that at least 32% of children between the ages of 10 and 17 in Bangladesh, are vulnerable to online violence, cyberbullying, and digital harassment (Nabi, 2019). This increasing number of cyberbullying incidents should not be taken lightly since it has tendency to cause dreadful consequences on the victims. For instances, Tyler Clementi, Asher Brown, Billy Lucas, Phoebe Prince and Seth Walsh have committed suicide after experiencing bully through the Internet (Wolf, 2012, p. 845). In 2006, Megan Meier hanged herself to death after her friend's mother Drew impersonated as a

ISSN: 2005-4238 IJAST

fictitious boy on the Internet and then sent her offensive online messages. Drew was then indicted and convicted for violating the Computer Fraud and Abuse Act in 2008 which was eventually reversed on appeal (McCarthy & Michels, 2009).

In 2010, Phoebe Prince committed suicide after being bullied in real life and bullied through the Internet. Later 6 teenagers were charged for criminal offences which ranged from statutory rape, stalking and assault with a deadly weapon (Hayes. 2014, p. 444). In May 2011, 5 of the bullies pleaded guilty to harassment and were sentenced for probation and community service and a charge for statutory rape against a male teenager was dropped (Mann, 2011).

In the same year of the death of Phoebe Prince, Tyler Clementi, a gay student who was studying in Rutgers University also committed suicide after his roommate, Ravi Dharun and his classmate, Molly Wei videotaped his sexual intercourse activities with another man and then streamed on the Internet (Jaffe, 2011, p. 382-383). Ravi was then convicted for 15 counts of invasion of privacy, bias intimidation, tampering with evidence, witness tampering, and hindering apprehension or prosecution (DeMarco, 2012).

These cyberbullying incidents seems to be very perilous to youngster as it is very harmful to victim's psychology. However, many countries have not yet enacted a specific legislation on cyberbullying including Malaysia where cyberbullying is handled mostly by Computer Crime Act 1997, Digital Signatures Act 1997, Communication and Multimedia Act 1998 and Penal Code among others.

2. Problem Statement

Problem of cyber threats against children is regarded as a serious issue in many countries including Malaysia although initially the issue was not as rampant as in some other countries but it was on a rise (CyberSecurity Malaysia, 2011). A 2018 survey conducted among 28 countries shows Malaysia is now sixth-worst in global cyberbullying ladder and second worst in Asia (Rosli, 2018).

According to Malaysian CyberSecurity (2010), 60 cases of cyberbullying in schools were reported in 2007 and the number is expected to grow (Masrom, Mahmood, Zainon, Wan, & Jamal, 2012, p. 506). This prediction of increasing number of incidents involving cyberbullying seems to be correct since in 2009, Cybersecurity Malaysia received about 174 complaints on online harassment and cyber stalking compared to 72 in the previous year (CyberSecurity Malaysia, 2010). Besides, a total number of 389 cyber-bullying reports were lodged by Internet users to the Cyber999 Help Centre in 2013 relative to previous year's 250 incidents showing a clear escalation of the incidents. In addition, the Global Youth Online Behavior Survey released by Microsoft Corp, which was conducted from 11 January to 19 February 2012, found that 2508 of 7,600 Malaysian children age of 8 to 17 who responded to the survey said that they had been subject to a range of online activities that some may consider to be online bullying (Digital News Asia, 2012).

There are several incidents of cyberbullying that ended up with teenager suicide. In 2011, a Malaysian teenager committed suicide after posting her intention to commit suicide on Facebook following a relationship breakup. She died after falling from the corridor of her school. Subsequently it was revealed that she was seriously disturbed due to some of the comments her Facebook status attracted from her online friends (Carvalho, Hamid, Foong, Kammed, & Tan, 2011). Again, a 12 years old Florida girl committed suicide by jumping from a platform at an abandoned cement plant after being received ruthless cyberbullying from other girls (Morgan & Roberts, 2018). Similarly, in Canada, a 15 years old girl, Amanda Todd, hanged herself in her home after being bullied online by her friends. The cyberbullying started after her online friend created a Facebook account and used her topless picture on the profile (Fong, 2012). These cyberbullying incidents has called for immediate attention from the governments.

ISSN: 2005-4238 IJAST

Apart from the growing number of incidents involving cyberbullying, its consequences to the victims are also very harmful. Hence, it should not be taken lightly. From the past, it can be seen that the cyberbullying has led victims to commit suicide. These incidents have led to many outcries for beefing up the laws and regulations due to the growing number of tragic incidents of cyberbullying across the world.

Last but not least, the non-existence of Act which specifically dealing with cyberbullying among children might attributes to the laxity of the law enforcement. Cyberbullying against Malaysia is governed by various laws such as Communications and Multimedia Act (CMA) 1998 and Penal Code. However, the existing legislations which dealing with cyberbullying may be inadequate to curb this issue due to the fast pace of the IT.

Methodology

This project paper is a doctrinal legal research. It only studies on the legal aspects and problems relating to the laws on cyberbullying. It does not seek to study on the sociological aspects. As such, this proposed legal research only adopting qualitative approach. This type of research is also known as armchair research, purely based on library using both primary and secondary sources of information. For instances, the primary sources of this project paper includes, but not limited, to Federal Constitution of Malaysia, Computer Crime Act 1997, Communication and Multimedia Act 1998, Penal Code, Child Act 2001 and decided cases. While the secondary sources include reference to books, articles, commentaries and newspaper either from online journal and hardcopies.

Forms of Cyberbullying against Children

According to Willard (2007), there are seven forms of cyberbullying which are flaming, harassment and stalking, denigration, impersonation, exclusion, outing and trickery. Flaming refers to a heated short-lived event which involves offensive, rude, insult, vulgar language and may also involving threats. The flame erupts between persons who arguing and insulting each other. The events usually take place in chat rooms, games and discussion boards. Denigration is a harmful, cruel and untrue speech about his target person. The purpose of spreading rumours and posting gossips about a person is to destroy reputation of the target or destroy their friendships. Defamation is a form of cyberbullying and it is most frequently used by students against teachers or other school employees. A student or a group of students embarrass the teachers or the school administrator by posting untrue comments about them in a blog or discussion group. This type of speech constitutes defamation or invasion of privacy. However, in an American case of *Finkel v. Dauber*, 2010 NY Slip Op 20292 [29 Misc 3d 325], the Supreme Court of Nassau County held that there is no cause of action for defamation accrued from the posting, and the submission by the plaintiff that the post constitute cyber bullying also rejected by court since cyber bullying is not recognised as "a cognizable tort action".

As for harassment, it is repeated, ongoing sending of offensive messages to an individual target. Harassing messaging generally sent via instant messaging, email and text messaging. Cyber harassment is not short-lived event. It occurs for some period of time where the perpetrator keeps sending offensive messages. Unlike flaming, cyber harassment is mostly one sided where the perpetrator is the one who keeps harassing the victim. Cyber stalking refers to repeatedly sending threats of harm or highly intimidating or extremely offensive messages which may even involve extortion, while impersonation refers to the act of pretending to be the target and post material that will embarrass the target or interfere with the target's friendship. Usually, the exchange of password gives an opportunity to a cyber-bully to gain access to the victim's account and impersonate as the victim. Exclusion usually refers to a group of individuals who gang up to outcast the victim from the online group or online buddy-list. For example, a boy who lost in the online game battle was threatened and out casted by his friends on the online game site. Outing and trickery refer to the act of tricks to obtain private information about the victim and then

forwarding private messages or post it to the public. For example, a girl asked her friend who does she like best, Jack or Nathan. The victim answered the question via instants messenger. The victim's IM was then made into public by her friend.

To sum, the tremendous expansion of internet coverage across the world gives a lot of impacts in human life. The methods of working, business, teaching and learning somehow have changed due to the dependency of internet in their life.

Children in Malaysia are also encouraged to learn about Internet. It is in line with the government's goal to produce computer literate nation. For instance, the launching of Smart School in Malaysia in 1997 is a manifestation of the government to encourage children to learn Information Technology (IT). However, the Internet is not entirely beneficial to children since there are many Internet users who willingly take advantage on children. The traditional methods to commit offences have now upgraded into new sophisticated methods where the perpetrators can easily commit cybercrimes without revealing themselves.

Cyberbullying among children in cyber space are undeniably very harmful to children even though there is no physical contact involved. The fact that cyberbullying may easily affect children's inner development compared to adult exacerbates this issue.

3. Overview of Cyberbullying

Cyberbullying is regarded as a complex multi-dimensional phenomenon (Kyriakides, Kaloyirou & Geoff, 2006) with negative consequences caused due to the acts of cyberbullying. The growing number of tragic incidents due to conducts of cyberbullying has caused anxiety to society. According to Juvonen and Gross (2008), people, especially parents, may seem to be frightened by cyberbullying phenomena since it engaged with communication technologies which are unfamiliar to them.

Hence, there are many countries have looked into this undesirable phenomenon and attempting to beef up the laws in order to halt the cyberbullying among children before it turns into catastrophic. However, there is not much known about the insidious of cyberbullying even though the international researches have been focusing on the phenomenon of bullying in schools for many years (Sakellariou, Carroll & Houghton, 2012, p. 534), and there has always been a challenge of defining cyberbullying which has limited our understanding of the issue in the first place, as observed by Barlett (2019, p.9). As such, it is important to discuss on the nature and consequences of cyberbullying.

4. Definition and Concept of Cyberbullying

In general, there is no a universal definition of cyberbullying. The cyberbullying has been defined by various scholars according to their understanding. Willard defines cyberbullying as "sending or posting harmful or cruel text or images using the Internet or other digital communication devices (Willard, 2003)". Later, cyberbullying was defined by Shariff and Strong-Wilson as comprising "covert psychological bullying, conveyed through the electronic media such as cell phones, weblogs and web sites, online chat rooms, MUD rooms (Multi User Domains where individuals take on different characters) and Xangas (online personal profiles where some adolescents create lists of people they do not like)" (Shariff, 2008). This definition seems to be more comprehensive than the definition provided by Willard.

Furthermore, cyberbullying was also defined as an aggressive, intentional and repeated act by individuals or a group of individuals via the usage of electronic forms of contact against a victim (Slonje & Smith, 2008). This definition is quite similar to the definition given by David-Ferdon, Hertz, Kowalski and

Limber who also view that cyberbullying consist of repeated act with intention to cause harm or emotional distress (Sakellariou, Carroll & Houghton 2012). Besides, there are also many other definitions that emphasize the element of intentional and repetitiveness act of cyberbullying. According to Hinduja and Patchin (2014), cyberbullying is a "willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices." Even though the definition is not a comprehensive definition, it encompasses four main components of the meaning of cyberbullying which are (1) deliberate or intentional conduct, it is not occurred accidentally; (2) repeated conduct, it is not occurred in a single event or incident; (3) there is a harm caused to victim according to the victim's perspective and (4) the act was done via a technological means (Hinduja & Patchin, 2014).

As mentioned previously, there is no universal definition of cyberbullying. This may cause several difficulties in appreciating the true nature of cyberbullying. For example, even though the "cyberbullying" is commonly used for students or juveniles, it is uncertain which party of cyberbullying should be minor (Schwartz, 2007). Some scholars contend that the victim and the perpetrator of cyberbullying should be minor as the cyberbullying is regarded as a counterpart of traditional bullying (Schwartz, 2007) while some other scholars argued that cyberbullying should refer to minor offender only regardless of the age of victim (Ruedy, 2008). The latter includes situations where children cyberbully their teachers. Last but not least, there are scholars suggest that the cyberbullying should refer to minor victims regardless of the age of the perpetrator (Ruedy, 2008). Thus, it is widely agreed that cyberbullying should only relate to children whereas cyber harassment and cyber stalking are adult's offences even though there is confusion as to which party should be minor.

Furthermore, the definitions also create haziness as to the categories of cyberbullying. The term "cyberbullying always used interchangeably with the terms "cyber harassment," and "cyber stalking,". There are definitions for cyberbullying that draw on some related concepts such as cyber stalking and online youth gangs. For example, Akbulut (2010) views that there are several categories of cyberbullying which are flaming, harassment, cyber stalking, denigration, masquerading, exclusion, outing and trickery. These forms of cyberbullying are similar with the forms of cyberbullying as suggested by Willard (2007). Hence, the forms of cyberbullying are quite fuzzy especially when it comes to whether or not the cyber stalking should be regarded as a form of cyberbullying. According to Andrew Murray (2013), harassment is "behaviour intended to disturb or upset" whereas stalking refers to "aggravated form of harassment where victim finds themselves followed and continually contacted by the offender". It is also interesting to note that some laws distinguish cyber stalking from cyber harassment in which it is necessary to prove credible threats whereas some laws did not make any distinction between cyber stalking and cyber harassment and thus, it is not required to prove credible threats (Schwartz 2009).

By looking at these definitions, it appears that many scholars highlight the element of repetitive in the definitions of cyberbullying. For example, Hinduja and Patchin (2015) defined cyber-bullying as "willful and repeated harm inflicted through the medium of electronic text". This element of repetitiveness is actually commonly used for traditional bullying.

From a legal standpoint, cyberbullying is frequently equated with harassment. This means that there must be a course of conduct which amounts to harassment of another person. Nevertheless, a single offensive or defamatory text is already sufficient to be considered as unlawful conduct regardless whether or not it is widely spread in the public. This is because tarnishing one's reputation is already considered as an infringing act. This unlawful conduct is, however, not specifically dealt by laws as offence of cyberbullying but dealt as other type of offences such as criminal defamation under Penal Code or CMA 1998.

Some countries have enacted laws that specifically deal with the offence of cyberbullying. In U.S, there are several states that expressly prohibit cyberbullying. For example, in Arkansas, cyberbullying is

considered as an offence under 5-71-217 of Arkansas Code. In Massachusetts, section 370(a), Chapter 92 of the *Acts* of 2010, defines cyberbullying. However, in some countries, laws are enacted to cover a very wide range of offences relating publications and sending of false and fear inducing data or information without clearly defining cyberbullying or harassment. For example, section 25 of the Digital Security Act 2018 (Bangladesh) says that

[i]f any person in any website or through any digital medium- (a) [i]ntentionally or knowingly sends such information which is offensive or fear inducing, or which despite knowing it as false is sent, published or propagated with the intention to annoy, insult, humiliate or denigrate a person or (b) [p]ublishes or propagates or assists in publishing or propagating any information with the intention of tarnishing the image of the nation or spread confusion or despite knowing it as false, publishes or propagates or assists in publishing or propagates information in its full or in a distorted form for the same intentions, [t]hen, the activity of that person will be an offense under the Act.

This law does not criminalise cyberbullying or harassment, and there is no mentioning of age of the victims and perpetrators involved. This broad legal provision run the risk of either being too ineffective due to its apparent vagueness or too partial due to its all-encompassing character. In short, the law leaves enormous power in the hands of prosecutors, which may eventually be abused to harass political opponent than serving any real purposes.

Similar approaches are there in Malaysian laws as well, specially section 233 (1) (a) of CMA 1998 may well be accused of being potential tools of abuse. In December 2015, former President of Malaysian Bar expressed his deep concern about this section in a press release and mentioned the provision should be repealed (Thiru, 2015). The press release cited several examples of persons and entities being charged under this provision. Besides, the Malaysia Human Rights Report 2016 published incidents where individuals were punished under this law based on their online comments including tweeting (SUARAM, 2016). Till date, however, nobody has yet been charged with cyberbullying under this law although its wider scope would easily permit such application.

Hence, it is our contention, in the absence of a universal definition of cyberbullying, that cyberbullying is an act of harassing, defaming or even threatening by a child or a group of children towards another child. As for definitions and forms of cyberbullying given by some scholars which include cyber stalking as a form of cyberbullying, it seems that cyber stalking is unsuitable to be considered as a form of cyberbullying since cyber stalking usually refers to unlawful conducts that follow or stalk a person for over some period which later cause fear to that person. Hence, it is better for legislature to provide legal definition for cyberbullying in order to avoid confusion.

5. Cyberbullying v Conventional bullying

Cyberbullying, basically is a new form of bullying which takes place on the Internet. This new form of bullying can be distinguished from the conventional bullying in several ways. Firstly, unlike traditional bullying, cyberbullying can be perpetrated anonymously (Rodkin & Fischer, 2012), because generally there is no obligation on the part of the Internet service provider to disclose the true identity of internet users when they are using the Internet. This advantage provided by the Internet allows cyber bullies to seek refuge behind the cloak of anonymity and continue bullying as they remain unaware of the impact of their harmful conducts against their victims (Erdur-Baker, 2010).

Then again, cyberbullying would allow more audiences than conventional bullying to the bullying incidents resulting a higher degree of victims' torment involving more violent or embarrassing actions towards the victims. Thirdly, the cyberbullying does not require the perpetrator to have a stronger physical built or physical strength (Erdur-Baker, 2010) to fight or make any physical contacts to the

victims. Fourthly, the cyberbullying is more ubiquitous compared to conventional bullying in today's era (Rodkin & Fischer, 2012, p. 621). The Internet, in a way, facilitates cyberbullying since it provides a platform where the cyber bullies can bully their victims without being restricted to any locations and any particular time.

Thus, the cyberbullying differs from conventional bullying as it entails a unique characteristic which is anonymity. This anonymous status of the internet users would not only cause less fear to the internet users to commit cyberbullying but also would cause hardship to the law enforcement agencies to find the perpetrators. Besides, the involvement of large audiences in cyberbullying incidents would cause devastating consequences to the victims. As such, cyberbullying should be regarded as a serious bullying issue.

Constitutional Guarantee of Freedom of Speech and Expression

Freedom of speech and expression is enshrined in Article 10 (1) (a) of the Federal Constitution of Malaysia. However, this right is subjected to clauses (2), which mentions that Parliament is allowed to impose restrictions by law on freedom of speech and expression "as it deems necessary or expedient" for the interest of the security of the Federation or any part thereof or public order. Here, the words "as it deems necessary or expedient" indicate that the Parliament has exclusive power to impose legislative restriction in this regard. Hence, the courts of law could not ascertain the expediency and necessity of the impugned restriction (Rodkin & Fischer 2012, p. 288).

This approach of ascertaining the validity of legislative restrictions on freedom of speech and expression is different from Bangladesh, for instance, the Supreme Court of Bangladesh is allowed to decide whether the impugned law that restricts the freedom of speech is reasonable (Rodkin & Fischer 2012, 287-288). Under Article 39 (2) (a) of the Constitution of the People's Republic of Bangladesh freedom of speech is a fundamental right and in case of any violation of this right anyone can move the High Court Division of the Supreme Court {Article 44 (a) and 102 (1)}. Besides, article 26 (2) prohibits enactment of any law inconsistent with any provisions of fundamental rights. As such, the Malaysian laws are still valid even the laws unreasonably restrict the freedom of speech.

However, let it be forgotten, the Malaysian courts have now followed different approach in determining the validity of law in restricting the constitutional rights. In the case of *Muhammad Hilman Bin Idham & Ors v Kerajaan Malaysia & Ors,* (MLJU 2011, p. 768) the Court of Appeal followed the Federal Court's approach in case of *Sivarasa Rasiah v Badan Peguam Malaysia & Anor* (MLJ 2010, p. 333) that the prohibition on university's students to express support or sympathy of political party as imposed by Section 15(5)(a) of the University and University College Act 1971 is a reasonable legislative restriction.

The restrictions can be imposed on the freedom of speech and expression for eight grounds. For instance, security of federation or any part thereof, friendly relations with other countries, public order, morality, privileges of Parliament or of any legislative assembly, contempt of court, defamation and incitement to any offence.

Thus, the freedom of speech and expression is not an absolute right. The constitution allows the Parliament to enact law based on several grounds. The new approach adopted by Malaysian court in deciding on the matters relating to constitutional rights also seems to be more just as the Parliament could not simply enact laws that unreasonably restrict the scope of freedom of speech.

This would also allow the legislature as well as the judiciary to strike for balance of public interest and individual's freedom of expression. As such, freedom of speech is not a defence to cyberbullying.

6. The Laws on Cyberbullying in Malaysia

In absence of any specific legislation, there are some provisions from various statutes that can be used to fight cyberbullying.

Communication and Multimedia Act 1998

In regards to cyberbullying, the relevant provisions in the CMA 1998 are Section 211 and 233 as mentioned earlier. However, section 211 is relevant for intermediaries whereas section 233 is applicable for end users. Broadly speaking, Section 233 of the CMA 1998 deals with improper use of network facilities. This section may be relevant to punish the perpetrator of cyberbullying. Sub-Section(1) prohibits a person who knowingly improperly uses network facilities or network service or applications service, either by initiating the transmission of any comment, request, suggestion or other communication which is obscene, indecent, false, menacing or offensive in character; or initiates a communication using any applications service, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his identity. Both *actus reus* must be coupled with *mens rea* which is "with intent to annoy, abuse, threaten or harass any person at any number or electronic address".

In *PP v Rutinin Bin Suhaimin*, (2 CLJ 2013, p. 427) the Public Prosecutor appealed before the High Court against the Sessions Court's decision for discharging the accused for committing an offence under Section 233 of the CMA 1998 by posting offensive remark on the online visitor book of the homepage of the HRH Sultan of Perak. The court held that the remark was regarded as intended to annoy, abuse, threaten or harass any person regardless whether the victim was annoyed by the statement. According to the Ravinthran Paramaguru JC in *Rutinin* (2 CLJ 2013, p. 427), the two essential ingredients of this offence are that the perpetrator had made such communication via a network facilities or network service and that communication was done with "with intent to annoy, abuse, threaten or harass any person". Besides, the term "knowing" in this section indicates that intention is required (Radhakrishna 2013). Court took the same approach in *Pendakwaraya v Muslim bin Ahmad* (1 AMR 2013, p. 436), where the accused was charged for three offences under Section 233(1)(a) of the CMA for posting offensive comments on the Perak State Government Official Portal.

As such, the above-mentioned section may be applicable against cyber bullies, as the cyberbullying itself constitutes an offence of improper use of network facilities or network service by harassing another person online. This is because the act of cyberbullying involves improper use of network facilities or network service by sending offensive message with intent to harass or at least to annoy the victim. However, the question is what if the perpetrator of cyberbullying did not actually intend to harass or to annoy the victim but merely intended it as a joke. Thus, the difficulty in prosecuting cyber bullies for the offence under Section 233 of the CMA 1998 is to prove the *mens rea* of the offence i.e, criminal intent. It also must be borne in mind that children or young people are susceptible to the culture or practice portrayed by the television or online social media. Their immaturity may lead to communicate with their peers in improper manners without any intention to annoy or harass them. As such, it is crucial for the court to take into consideration the age of the perpetrator, the content of the alleged statement and the closeness of the relationship between the perpetrator and victim in ascertaining the *mens rea* of the perpetrator.

Penal Code

The offender of cyberbullying may also be charged for criminal intimidation (Section 506). The essential ingredients of this offence are threatening the victim with any injury to the victim and intent to cause harm to the victim (7 MLJ 2005, p. 57). This indicates that this offence, as most of other criminal

offences, is required to establish the element of *actus reus* and *mens rea* (2 CLJ 2003, pp. 559-560). In *Sinnasamy A/L Kaliappan v Public Prosecutor*, the High Court held that producing weapon is not necessary to establish criminal intimidation as mere words would suffice for the offence. Besides, the words in this context do not necessarily refer to spoken words only but also include written words. In *Queen Express v Mangesh Jiva'ji* (11 ILR Bom 1887, p. 376), the accused was charged under Section 507 of the Indian Penal Code for sending a fake petition to Revenue Commissioner containing a threat stating that unless Mr. MacGregor, Forest Officer who fired the accused person from his job, were transferred to some other district, he would be killed. However, the Appellate Court reversed the conviction because of lacking of an ingredient of that offence since the person to whom the petition was sent by the accused person was not himself threatened, and not "interested" in the person threatened. As such, the accused also could not be convicted for attempt of which he had been convicted (11 ILR Bom 1887, p. 376). Thus, the perpetrators of cyberbullying who post a threat on the internet to cause injury or send e-mail containing such threats to their victims may be charged under Section 506 of the Penal Code for criminal intimidation.

Furthermore, the offenders for criminal intimidation by an anonymous communication may be charged under Section 507 and be punished in addition to the punishment provided for the offence by Section 506. Besides, perpetrators of cyberbullying can also be liable under Section 509 of the Penal Code if they utter any word, make any sound or gesture or exhibit any object so that the victim can see or listen or even intrude upon the privacy of such person in order to insult the modesty of a person. This provision may equally be applicable for offences committed online as well.

7. Regulatory Framework on Cyberbullying in School

The main legislation that governs matters relating to schools and is Education Act 1996. The Minister may enact regulations on certain matters, which have been stated in the Act (section 130). Besides, Director General of Education may also issue Professional Circulars, which are commonly referred as "*Surat Pekeliling Ikhtisas*", in compliance with the regulations and the Act, and then the school principal may design school regulations and enforce them accordingly.

In "*Surat Pekeliling Ikhtisas bil. 8/2010*: Guidelines on prevention and dealing with bullying among pupil in school", the circular states that action may be taken against students who commit bullying in school or hostel. The principal or authorised teachers may impose penalties such as issuing warning letter, prohibit the offender from using the school's facilities, prohibition from using hostel's facilities, caning not exceeding three strokes, suspension from school up to 14 days or expel from the school, depending on the seriousness of the bully.

However, the circular does not explicitly state that it also regulates cyberbullying. Nevertheless, it contended by the authors that it does cover and regulate cyberbullying since the word "bully" is wide in meaning and may also cover cyberbullying. Moreover, there are others circulars dealing with issues relating student's discipline, for instance, prohibition on students bringing mobile phone in school . These disciplinary rules and their strict enforcement may help prevent cyberbullying to some extent but cannot fill the gap of specific legislation criminalising cyberbullying in the national level.

8. Recommendation and Conclusion

In order to enhance the law and protection against cyberbullying, few suggestions here may be useful.

Firstly, the existing legislations on cyberbullying can be amended or new piece of legislation can be enacted to provide cyberbullying a comprehensive definition of cyberbullying with enough punitive measures so that appropriate charge can be framed against the perpetrator of cyberbullying. The proposed

legislation may be modelled on legislations of jurisdictions where anti-cyberbullying laws are being successfully implemented.

Besides, Malaysia may also consider Protection from Harassment Act 1997 as enforced in the UK or as in Singapore (The Protection from Harassment Act 2014) which cover both cyberbullying and cyber stalking.

To sum, children's online safety should be given a paramount consideration since children are exposed to many risks online. There are several categories of online privacy and security related risks, especially, cyberbullying which has devastating effect on children. The legislature in Malaysia should have clear law in place relating cyberbullying in order to avoid confusions on the real concept of cyberbullying and to safeguard children in the cyber space.

References

[1] Akbulut Y, Sahin Y. L. & Eristi B, (2010). 'Cyber-bullying among Turkish online social utility members', *Educational Technology & Society*, vol. 13, no. 4, 192–201.
[2] Anis N. M. N., Rahim R. A., & Lim, Y. (2012). '*Najib: Cyber bullying a serious threat to kids'*. Available at: https://www.thestar.com.my/news/nation/2012/10/10/najib-cyber-bullying-a-serious-threat-to-kids (Accessed: 4 August 2019).
[3] Ayub, Z.A., Yusoff, Z.M. (2018). 'Right of Online Informational Privacy of Children in Malaysia: A Statutory Perspective', *Universiti Utara Malaysia Journal of Legal Studies (UUMJLS)*, vol.9, no.1.
[4] Barlett, C. P. (2019). *Predicting Cyberbullying: Research, Theory, and Intervention.* London, UK: Academic Press.
[5] Carvalho M., Hamid R. A., Foong J., Kammed K. A., and Tan C. (2011). '*Girl kills self after Facebook post'*. Available at: https://www.thestar.com.my/news/nation/2011/02/09/girl-kills-self-after-facebook-post/ (Accessed: 5 August 2019).
[6] CyberSecurity Malaysia. (2010). *'Cyberstalking a serious threat'*. Available at: https://www.cybersecurity.my/en/knowledge_bank/news/2010/main/detail/1853/index.html (Accessed: 5 August 2019).
[7] CyberSecurity Malaysia. (2011). '*Keeping children cyber-safe'*. Available at: https://www.cybersecurity.my/en/knowledge_bank/news/2011/main/detail/2114/index.html (Accessed: 4 August 2019).
[8] DeMarco M. (2012). '*Live coverage: Dharun Ravi found guilty on most counts in webcam spying trial verdict'*. Available at: http://www.nj.com/news/index.ssf/2012/03/ravi_webcam_trial_verdict.html (Accessed: 4 August 2019).
[9] Digital News Asia (2012) '*1-in-3 Malaysian kids victims of cyber-bullying: Microsoft survey'*. Available at: https://www.digitalnewsasia.com/testing123 (Accessed: 5 August 2019).
[10] Erdur-Baker O. (2010). 'Cyberbullying and its correlation to traditional bullying, gender and frequent and risky usage of internet-mediated communication tools', New *Media & Society,* vol. 12, no. 1, 109-125.
[11] Fong P. (2012). '*B.C. victim of cyber-bullying commits suicide*'. Available at: http://www.thestar.com/news/canada/2012/10/12/bc_victim_of_cyberbullying_commits_suicide.html (Accessed: 5 August 2019).
[12] Hayes, D. R. (2014). *A Practical Guide to Computer Forensics Investigations*. Indiana: Pearson IT Certification.
[13] Hiichiikok Foundation. (2013). '*Our stand against cyber crimes against children'*. Available at: http://hiichiikokfoundation.com/index.php/updates/9-events/77-our-stand-on-cybercrime-against-children (Accessed: 4 August 2019).

[14] Hinduja, S. & Patchin, J.W. (2014). *Cyberbullying: Identification, Prevention, & Response.* Available at: https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response.pdf (Accessed: 18 August 2019).
[15] Hinduja, S. & Patchin, J. W. (2015). *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying* (2nd edition). Thousand Oaks, CA: Sage Publications.
[16] Jaffe, E.M. (2011). 'Cyberbullies Beware: Reconsidering Vosburg v. Putney in the Internet Age', *Charleston Law Review*, no. 5, pp. 382-383.
[17] Jalil J.A. (2011). 'Children and the Internet: Beware of the Threats from Within', *The Law Review*. 210.
[18] Juvonen, J., and Gross, E. F. (2008). Extending the school grounds? Bullying experiences in cyberspace. *Journal of School Health*, no. 78(9), p. 497.
[19] King, A.V. (2010). Constitutionality of Cyberbullying Laws: Keeping the Online Playground Safe for Both Teens and Free Speech. *Vanderbilt Law Review*, no. 63, p. 846.
[20] Kyriakides L., Kaloyirou C., & Geoff. (2006). An analysis of the Revised Olweus Bully/Victim Questionnaire using the Rasch measurement model. *British Journal of Educational Psychology*, no. 76(4), pp. 781–801.
[21] Mann, C. (2011). *Rape charge dropped in Phoebe Prince Mass. bully-suicide case, five others plead guilty to harassment*. Available at: http://www.cbsnews.com/news/rape-charge-dropped-in-phoebe-prince-mass-bully-suicide-case-five-others-plead-guilty-to-harassment/(Accessed: 4 August 2019).
[22] Masrom M, Mahmood N, Zainon, O, Wan, HL and Jamal, N. (2012). Information and Communication Technology Issues: A Case of Malaysian Primary School. *ARPN Journal of Science and Technology*, 2 (5) p. 506. Available at: https://pdfs.semanticscholar.org/7df0/5b74cbd1941fbaa7dddd370934120e40ffc5.pdf. (Accessed: 15 August 2019).
[23] McCarthy, T., & Michels, S. (2009). *Lori Drew MySpace Suicide Hoax Conviction Thrown Out'*. Available at: http://abcnews.go.com/TheLaw/story?id=7977226 (Accessed: 10 March 2014).
[24] Morgan, C., and Roberts, A. (2018). *Twelve-year-old girl commits suicide after cyber-bullying*. Available at: https://www.thesun.co.uk/fabulous/7609464/mallory-grossman-suicide-12/ (Accessed: 5 August 2019).
[25] Murray, A. (2013). *Information Technology Law: The Law and Society*. 2nd edn. Oxford: Oxford University Press.
[26] Nabi, M. S. (2019). *Unicef: 32% kids at risk of cyberbullying in Bangladesh'.* Available at: https://www.dhakatribune.com/bangladesh/dhaka/2019/02/05/unicef-prevent-online-bullying-harassment-of-children-in-bangladesh (Accessed: 18 April 2019).
[27] Patel, K. A. (2011). Cyberbullying: What's the "Status" in England? *San Diego International Law Journal*, no. 13, p. 590.
[28] Radhakrishna, G. (2013). Legal Presumptions and the burden of proof: S.114A Evidence (Amendment) (No.2) Act 2012. *CLJ Legal Network Series*, 1 LNS Ixxxv: 4.
[29] Rodkin P. C, & Fischer K. (2012). Cyberbullying from Psychological and Legal Perspectives. *Missouri Law Review*, vol. 77, no. 3, p. 621.
[30] Rosli, J. (2018). *Malaysia sixth-worst in global cyber-bullying ladder, survey shows.* Available at: https://www.malaymail.com/news/malaysia/2018/10/27/malaysia-sixth-worst-in-global-cyber-bullying-ladder/1687181 (Accessed: 3 September 2019).
[31] Ruedy, M.C. (2008). Repercussions of a MySpace Teen Suicide: Should Anti-Cyberbullying Laws Be Created? *North Carolina Journal of Law and Technology*, no. 9 (2), p. 326.
[32] Sakellariou T., Carroll A., & Houghton S. (2012). Rates of cyber victimization and bullying among male Australian primary and high school students. *School Psychology International*, no. 33(5), p. 534.

[33] Schwartz, K.E. (2009). Criminal liability for internets culprits: the needs for update state laws covering the full spectrum of cyber victimization. *Washington University Law Review*, vol. 87, no. 2, pp. 410-411.
[34] Sellgren, K. (2014). '*Cyberbullying 'on rise' – ChildLine'*. Available at: http://www.bbc.com/news/education-25639839 (Accessed: 4 August 2019).
[35] Shariff, S. (2008). *Cyber-Bullying*. London: Routledge.
[36] Slonje R., & Smith P. K. (2008). Cyberbullying: Another main type of bullying? *Scandinavian Journal of Psychology*, no. 49, pp. 147–54.
[37] SUARAM. (2016). *Malaysia Human Rights Report 2016: Civil and Political Rights.* Edited by Kua Kia Soong and James Lochhead. Selangor: Suara Inisiatif Sdn Bhd.
[38] Thiru, S. (2015). *Press Release | Section 233(1)(a) of the Communications and Multimedia Act 1998 Creates a Chilling Effect on Freedom of Speech and Expression, and Should be Repealed.* Available at:http://www.malaysianbar.org.my/press_statements/press_release_%7C_section_2331a_of_the_communications_and_multimedia_act_1998_creates_a_chilling_effect_on_freedom_of_speech_and_expression_and_should_be_repealed.html (Accessed: 18 August 2019).
[39] Willard, N. (2003). Off-campus, harmful online student speech. *Journal of School Violence*, vol. 1, no. 2, p. 66.
[40] Willard, N. E. (2007). *Cyberbullying and Cyberthreats : responding to the Challenge of Online Social Aggression, threats and distress*. Illinoi: Research Press.
[41] Wolf, J., (2012). The Playground Bully Has Gone digital: the Dangers of cyber bullying, the First Amendment Implications, and the necessary Responses. *Cardozo Public Law, Policy, and Ethics Journal*, no. 10, p. 845.