MALAYSIA'S APPROACH TOWARDS CYBER BULLYING: THE EXISTING FRAMEWORK

Win Li Low, The Honourable Society of Lincoln's Inn
Dihlvinder Kaur Gill, INTI International University

ABSTRACT

Society's increased use and dependence on social media platforms has led to the prevalence of cyber bullying incidents. Following a global uproar over an incident in 2019 where Instagram users voted in favor of a Malaysian teenager's death, which in turn led to greater pressure to examine the existing legislative framework in Malaysia and efficiency of safeguards in respect to online space. Aside from Malaysia, this paper explores statutes, cases, and recommendations implemented in other Commonwealth countries such as Singapore, Ireland and the United Kingdom.

Keywords: Cyber Bullying, Existing Legislative Framework Malaysia and Other Common -wealth Countries, Efficiency Safeguards and Recommendations

INTRODUCTION

Incidents of cyber bullying are not something new. Such incidents of bullying occur via the use of digital devices such as cell phones, computers and tablets. These include derogatory comments which are shared on social media platforms such as Facebook, Instagram, Twitter, TikTok - to name a few.

Given society's increased use and dependence on these platforms, the prevalence of cyber bullying incidents has increased as well as society's reliance and validation sought from online users. The ability to remain anonymous and conceal one's identity online is open to abuse, as it gives perpetrators power over their victims (Abdullah, 2020).

The importance of addressing cyber bullying was highlighted in 2019 when Malaysia made worldwide headlines when a sixteen-year-old Malaysian girl committed suicide after considering the responses of a poll posted on her Instagram page (Jamie, 2019). In her poll, her followers had to decide between "Death" or "Life", and 69% voted for "Death" (Nazari, 2020).

Following this incident, there were several discussions on the need to create awareness, as well as introducing appropriate legislation to discourage and prevent online abuse. As a result, a proposed bill was considered, however, the outcome of these discussions are yet to be disclosed (The Star Online, 2019). Unfortunately a year after this incident, another victim took her own life after receiving a barrage of derogatory remarks for a TikTok video that went viral (Basyir & Perimbanayagam, 2020). As at March 2021, it has been reported that the Communications and Multimedia Ministry is preparing a Cabinet paper on anti-cyber bullying laws (Malay Mail, 2021). As of August 2021, it was reported that the government is currently drafting these cyber bullying laws. Malaysia Cyber security Outreach and Capacity Building senior vice-president, Lt Col (R) Mustaffa Ahmad said with the specific laws, the prosecution process for cyber bullying would no longer be based on other acts, including Section 233 of the Communications and Multimedia Act 1988 which relates to improper use of network facilities where this section has been used to prosecute offences relating to cyber bullying which is the current practice.

Cyber Bullying in Malaysia

Citation Information: Low, W.L, & Gill, D.K. (2022). Malaysia's approach towards cyber bullying: The existing framework. *Journal of Legal, Ethical and Regulatory Issues, 25*(S2), 1-14.

According to a poll released by UNICEF and the United Nations Special Representative of the Secretary-General on Violence against Children, 28% out of 6953 of young people in Malaysia have reported being a victim of online bullying (#children4change, 2019).

A study was also conducted to identify cyber bullying activities among youths in Selangor. The study was based on the responses of a cross-sectional survey that measured cyber bullying engagement which was distributed among 400 youths across four districts. The study concluded that blocking others in instant messaging applications was one of the most common actions of cyber bullying. Ignoring (which is also referred to as 'ghosting'), condemning someone, using slang terms, instant messaging and threats to remove or ostracize someone from a group were recorded as some of the other forms of cyber bullying.

According to the Women's Centre for Change, aggressive online behavior of Malaysians mostly manifests itself in derogatory comments (The Sun Daily, 2020). Other forms of cyberbullying include outing someone, trickery, cyber stalking (Walker, A., 2009), flaming, impersonation and trolling (Ijachi, 2019).

It was recorded that from January to June 2020, the Malaysian Communications and Multimedia Commission (MCMC) had received a total of 11,235 complaints (Selangor Journal, 2020) covering a range of cyber offences such as hacking, gambling, promoting prostitution, exposing official documents, harassment, cyber bullying, distributing pornography, identity imposters, sharing personal pictures, fake news, hate speech, religious intolerance, extremism and insulting the royalty. Complaints of harassment also included bullying, sexual harassment, fear, misuse of personal information and photos to embarrass and humiliate individuals (Liew, 2020).

Aside from a lack of morality and social norms, another problem that arises is the lack of a specific legal framework in deterring cyber bullying. Some of the issues that need to be resolved include how cyber bullying should be defined given its broad spectrum. Should the law be codified, or is it sufficient for offences to be brought under existing laws on harassment or defamation? Additional factors that should be considered include the types of remedies which should be accorded to a cyber-bullying victim and clearly defined consequences that a perpetrator could face.

Malaysia's Existing Framework on Cyberbullying

According to a global advisory survey conducted by Ipsos, 75% of Malaysians believe that our local anti-bullying measures are presently insufficient (Ipsos, 2018). Continuous review of existing legislation affecting the use of social media should be undertaken.

The Communications and Multimedia Ministry appointed the Multimedia University (MMU) to conduct research on anti-cyberbullying laws (The Star Online, 2020). According to the former Communications and Multimedia Minister, Datuk Saifuddin Abdullah, he observed. "If we want to make cyberbullying a crime, we have to look at existing legislation… there may already be existing provisions. However we also need to study if existing laws are sufficient and if it is not, we will then decide if a specific Act is needed to address cyberbullying" (Bernama, 2020).

Currently there is no specific legislation on cyberbullying in Malaysia. However, there are existing laws that addresses online behavior which are referred to below:

Communications and Multimedia Act 1998

In October 2019, the Ministry of Health published an infographic that determined body-shaming as a cyberbullying crime (SAYS, 2019).

Citation Information: Low, W.L, & Gill, D.K. (2022). Malaysia's approach towards cyber bullying: The existing framework. *Journal of Legal, Ethical and Regulatory Issues, 25*(S2), 1-14.

Section 233 of the Communications and Multimedia Act (CMA) 1998 deals with the improper use of network facilities. This section provides and prohibits a person who knowingly or improperly uses network facilities, network services, 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.

Section 233 (1)(b) covers the sharing of any obscene, indecent, false, menacing or offensive content, with the intent to annoy, abuse, threaten or harass another person. Should the offender be found guilty, they can be fined no more than RM 50,000 or imprisonment for no more than a year, or both.

In both these sections the broad definition of what constitutes improper use could in turn lead to an abuse of power as these sections do not specifically address cyberbullying nor do they define the scope of the intention required to prove the commission of the offence.

As of November 2020, the MCMC stated that 48 court charges were filed against individuals for misusing social media from January to September 2020, this is a 66% increase from the previous year. Out of the 48 charges, 34 were listed as offences committed under Section 233 CMA (Yeoh, A., 2020). The remaining 14 charges were offences committed under the Penal Code and Sexual Offences against Children Act 2017.

Computer Crimes Act 1997

Section 3 of the Computer Crimes Act 1997 provides that a person shall be guilty of an offence if he causes a computer to perform any function with the intent to secure access to any program or data held in any computer, such access which he intends to secure is unauthorised and he knows at the time when he causes the computer to perform the function that this is the case. The intention of a perpetrator does not require specifying the program or data housed in the computer in order to show that there was indeed intent. A person guilty of an offence under this section shall on conviction be liable to a fine not exceeding RM 50,000 or to imprisonment for a term not exceeding five year or to both.

Section 4 states that a person shall be guilty if he commits an offence referred to in section 3, with intent to commit an offence involving fraud or dishonesty or which causes injury as defined in the Penal Code, or to facilitate the commission of such an offence whether by himself or by any other person. Section 44 of the Penal Code defines injury as "any harm whatsoever illegally caused to any person, in body, mind, reputation or property." (Penal Code (Act 574), s 44). The definition of injury again under the Penal Code is fairly wide.

Section 5 of the Act provides that a person shall be guilty of an offence if he does any act which he knows will cause unauthorized modification of the contents of any computer. Within these sections there is no specific reference to offences relating to cyber bullying.

Evidence Act 1950: Internet Publications

Section 114A of the Evidence Act 1950 places greater accountability on service providers to moderate the actions of their users. According to this section:

1) A person whose name, photograph or pseudonym appears on any publication depicting himself as the owner, host, administrator, editor or sub-editor, or who in any manner facilitates to publish or republish the publication is presumed to have published or re-published the contents of the publication unless the contrary is proved.

Citation Information: Low, W.L, & Gill, D.K. (2022). Malaysia's approach towards cyber bullying: The existing framework. *Journal of Legal, Ethical and Regulatory Issues, 25*(S2), 1-14.

2) A person who is registered with a network service provider as a subscriber of a network service on which any publication originates from is presumed to be the person who published or re-published the publication unless the contrary is proved.
3) Any person who has in his custody or control any computer on which any publication originates from is presumed to have published or re-published the content of the publication unless the contrary is proved.

Section 114A of the Evidence Act 1950 gives rise to the presumption that any internet posting is presumed to have been published by a 'real person' of said name, photograph or pseudonym. Content published by users of the network service will then be traced to the registered individual or entity responsible. Though there is a lack of precedent in applying Section 114A, its ambiguity raises the need for better safeguards to hold the actual user/users involved accountable (Thomas Philip Advocates & Solicitors, 2019).

Penal Code

Another alternative that was discussed to deal with cyberbullying is Section 506 of the Penal Code for criminal intimidation. The essential ingredients of this offence is threatening the victim with any injury, with the intent to cause harm to the victim. Furthermore, the offenders for criminal intimidation by anonymous communication may be charged under Section 507.

It is interesting to note that a questionnaire related to cyberbullying conducted by MMU found that 89% of legal practitioners agreed that cyberbullying should be categorised as a criminal offence (The Sun Daily, 2020).

Within Malaysia's current legislative scope there are several Acts that overlap and cover certain provisions which may or could amount to cyberbullying however the existing legislation is not sufficient in address offences relating to cyberbullying as a whole.

Considering Malaysia's common law legal system, neighboring countries have made inroads in implementing laws and the following section will explore the approaches taken by other countries in addressing cyberbullying.

Comparative Legislations in Other Jurisdictions

Singapore

The Protection from Harassment Act (POHA), was enacted in 2014 which was designed specifically to make cyberbullying, stalking and online harassment within and out of the workplace a criminal offence. Particularly, Section 3, 4, 5, and 7 provide as follows:

Section 3: Intentionally causing harassment, alarm or distress
An individual or entity must not with intent, cause harassment, alarm or distress to another. Examples of such actions can be by way of:

a) Threatening, abusive or insulting words or behavior;
b) Make any threatening, abusive or insulting communication; or
c) Publishing any identity information of the targeted person or a related person of the targeted person. An accused is able to defend their actions if it can be shown that their conduct was reasonable.

Section 4: Harassment, Alarm or Distress

An individual or entity, must not by any means

a) Use any threatening, abusive or insulting words or behavior; or

Citation Information: Low, W.L, & Gill, D.K. (2022). Malaysia's approach towards cyber bullying: The existing framework. *Journal of Legal, Ethical and Regulatory Issues, 25*(S2), 1-14.

b) Make any threatening, abusive or insulting communication, which is heard, seen or otherwise perceived by any person likely to be caused harassment, alarm or distress.

There are Two Elements to a Defence under this Section

The accused had no reason to believe that the words or behavior used, or the communication made, by the accused would be heard, seen or otherwise perceived by the victim; or it was reasonable.

Section 5: Fear, Provocation or Facilitation of Violence

An individual or entity must not by any means use towards another, any threatening, abusive or insulting words or behavior, or make any threatening, abusive or insulting communication to another person. This can take the form of

1) Intentionally causing the victim to believe that unlawful violence will be used by any person against the victim or any other person; or
2) To provoke the use of unlawful violence by the victim or another person against any other person. Alternatively where, the victim is likely to believe that such violence will be used or provoked.

Additionally, an individual or entity must not by any means publish any identifying information of another person or a related person of the victim, either

1) To intentionally cause the victim to believe that unlawful violence will be used against the victim or any other person; or
2) To facilitate the use of unlawful violence against the victim or any other person. Alternatively, where there is reasonable cause to believe that it will likely cause the victim to believe that unlawful violence will be used against the victim or any other person; or to facilitate the use of unlawful violence against the victim or any other person.

Section 7: Unlawful Stalking

An individual or entity must not unlawfully stalk another person. There are several examples of acts or omissions which are associated with stalking:

Following the victim or a related person;

a) Making any communication, or attempting to make any communication, by any means (i) to the victim or a related person;
b) entering or loitering in any place (whether public or private) outside or near the victim's or a related person's place of residence or place of business or any other place frequented by the victim or the related person;
    I. Relating or purporting to relate to the victim or a related person; or
    II. Purporting to originate from the victim or a related person

c) interfering with property in the possession of the victim or a related person (whether or not the accused has an interest in the property);
d) giving or sending material to the victim or a related person, or leaving it where it will be found by, given to or brought to the attention of the victim or a related person;
e) keeping the victim or a related person under surveillance.

The accused ought reasonably to know that the accused's course of conduct is likely to cause harassment, alarm or distress to the victim if a reasonable person in possession of the same information would think that the course of conduct is likely to have that effect.

Citation Information: Low, W.L, & Gill, D.K. (2022). Malaysia's approach towards cyber bullying: The existing framework. *Journal of Legal, Ethical and Regulatory Issues, 25*(S2), 1-14.

Defenses available to the accused under the Act include the following

a) That the accused had no reason to believe that the words or behaviour used, or the communication made, by the accused would be heard, seen or otherwise perceived by the victim;
b) That the accused's conduct was reasonable.
c) that the course of conduct was pursued under any written law or rule of law or to comply with any condition or requirement imposed by any person under any written law;
d) That the course of conduct was lawfully done under a duty or power under any written law for the purpose of preventing or detecting crime; or
e) That the course of conduct was done on behalf of the Government and was necessary for the purposes of national security, national defence or the conduct of international relations.
f) (These are paraphrased from Sections 3, 4, 5, and 7 POHA 2014)

The offence of "doxing" was later updated added in the Act. This refers to the publication of a victim's personal information with the intention of harassing, threatening or abusing them. Under POHA, a victim can apply for a protection order if they are a victim of any of the actions specified in the sections (including section 6, and the offence of doxing). To apply for a protection order, this can be filed online after completing a pre-filing assessment via the Community Justice & Tribunals System (CJTS) or via an originating summons (Singapore Legal Advice, 2021).

Other remedies outside this Act which have been considered include mediation, suing for defamation, criminal intimidation per section 503 Penal Code, and suing for the transmission of obscene images electronically per section 292 Penal Code (Wong, 2019).

Singapore's approach in dealing with cyberbullying serves as s good checklist on issues and offences that need to be addressed within any cyberbullying laws. POHA defines the scope of the different forms cyberbullying and manner in which a victim can protect themselves by obtaining a protection order The Act also provides for a threshold in respect to appropriate defenses and the consequences that perpetrators would be faced with.

A recent example of the application of POHA related offences occurred on the 7th July 2021, where a Singaporean teenager was sentenced for threatening to kill a Premier League (EPL) football player and his family. On three separate occasions, the teenager had sent threatening messages via anonymous social media accounts to the football player (The Straits Times, 2021). As a result of the teen's threats, the football player was left distressed. In accordance with Section 3 POHA, an offender could be jailed for up to 6 months and/or fined up to $5000. However, the teenager was sentenced instead to 9 months' probation with a good behavior bond.

United Kingdom

Although there are no specific laws addressing cyberbullying, there are several legislations used to prosecute cases involving online communications in the U.K. These include: Offences Against the Person Act 1861, Malicious Communications Act 1988, Crime and Disorder Act 1998 and the Serious Crime Act 2015 (Myers & Cowie, 2019). The Protection from Harassment Act 1997 as enforced in the U.K also covers cyberbullying and cyber stalking (Ayub et al., 2020). Other laws that have been considered include the Public Order Act 1986, the Education and Inspections Act 2006 (EIA 2006), the Telecommunications Act 1984, the Obscene Publications Act 1959, the Computer Misuse Act 1990, and the Defamation Act 2013.

The difficulty with prosecuting an offence of cyberbullying, is once again the lack of a specific statute that addresses such an offence. As there is no specific offence for this situation, prosecutors will need to make an initial assessment to decide what offence was committed before deciding on its criminality (Asam & Samara, 2016). A consideration of decided cases demonstrates this.

Citation Information: Low, W.L, & Gill, D.K. (2022). Malaysia's approach towards cyber bullying: The existing framework. *Journal of Legal, Ethical and Regulatory Issues, 25*(S2), 1-14.

In the case of Kellett *vs* DPP (2001), Kellett was convicted of harassment in accordance with section 2 of the Protection from Harassment Act 1997. Kellett had telephoned the complainant's neighbor's employer and made unproven allegations. Even though the complainant was informed of this by a third party, it did not mean that no offence had been committed (Kellett *vs* DPP (2001) EWHC Admin 107, para. 16). The element that has to exist is that "so long as there is evidence on the basis of which the court can properly conclude, that the appellant was pursuing a course of conduct which he knew or ought to have known amounted to harassment of the complainant."

Kellett's appeal was dismissed and his conviction upheld. The court concluded that it was both foreseeable and inevitable that the complainant would become aware of the complaints made and accordingly the court had been correct in its conclusion that Kellett had pursued a course of conduct which he knew or should have known would amount to harassment. Additionally, the allegations had gone far beyond genuine concern and public duty as they involved accusations of fraud and moreover there had been no error in the court's approach.

In R *vs* Debnath (2005), the defendant had carried out a campaign of harassment of the complainant and his fiancée for a year. Her actions included sending multiple emails to the complainant's fiancée, sabotaging the complainant's email account, setting up a website of fake allegations on the complainant's sexual practices and overall harassment.

Aside from section 2 of the Protection from Harassment Act 1997, the defendant also pleaded guilty to unauthorised modification of computer material under Section 3 of the Computer Misuse Act 1990 in pursuing an act intended to pervert the course of justice along with further offences under the Act.

The defendant argued that the restraining order imposed was a breach of the Human Rights Act 1998 Sch.1 Part I Art.10. In dismissing the appeal the courts took the view that the wide terms of the restraining order were necessary to prevent crime and to protect the complainant and his fiancée. It should be noted that the Court has the power to vary or discharge an order under section 5(4) of the Protection from Harassment Act. However in this case the Court of Appeal did not interfere with the terms of a restraining order as the terms were appropriate in the circumstances (Criminal Law Review, 2006). The restriction on the defendant's freedom had to be considered and balanced against the rights of the complainant. According to Article 8 of the European Convention on Human Rights, the complainant too is entitled to the protection of private and family life. In upholding the order the court concluded that the restraining order in this case was prescribed by law to further a legitimate aim which was necessary in a democratic society and proportionate (Lester, Pannick & Herberg).

Whilst the appeal was about the terms of the restraining order there was no argument raised that communication to those other than the actual victim could not in itself amount to harassment. Amendments to the Act now allow for restraining orders to be made available upon the acquittal of an accused in a criminal offence where the order is necessary to protect an individual from future harassment (Edwards, 2010).

Ireland

In February 2021 the Harassment, Harmful Communications and Related Offences Act 2020 (HHCR) was passed (Irish Examiner, 2021). This law had been campaigned for after Nicole Fox (Coco) took her own life as a result of having suffered physical and online abuse for years. This Bill was in recognition of those who had lost their lives or had been victims of online abuse. According to the explanatory memorandum for the Bill (Tithe an Oireachtais Houses of the Oireachtas, 2020), its primary purpose was to amend the law and create new offences in relation to harassment and harmful communications both online and offline.

Citation Information: Low, W.L, & Gill, D.K. (2022). Malaysia's approach towards cyber bullying: The existing framework. *Journal of Legal, Ethical and Regulatory Issues, 25*(S2), 1-14.

The Bill, as amended provides for two new offences to deal with the recording, distribution or publication of intimate images without consent and provides for the anonymity of victims in such offences. The Bill also provides for an offence involving the distribution, publication, sending of threatening or grossly offensive communications as well as messages with intent to cause harm without a requirement for persistence.

Prior to the introduction of the HHCR (also known as Coco's Law), there were a number of criminal law and educational law provisions and guidelines given to schools to address bullying and cyberbullying behaviour.

The Education and Libraries [Northern Ireland] Order 2003 was introduced to ensure that all schools would establish an anti-bullying policy. In terms of criminal law, there are three pieces of legislation which may provide protection from cyberbullying: The Protection from Harassment (Northern Ireland) Order 1997, Malicious Communications (Northern Ireland) Order 1988, and The Communications Act 2003 (Purdy, N., & Mc Guckin, C., 2015). It should however be noted that these Acts were not introduced for the specific purpose of dealing with cyberbullying.

With the introduction of HHCR this legislation bans cyberbullying, stalking and sharing intimate images online without consent (Mirror, 2020). This law provides that a person who intentionally or recklessly, and without lawful authority or reasonable excuse:

- Persistently follows, watches, pesters or besets another person, or
- Persistently communicates with another person, or
- Persistently communicates with a third person about another person, is guilty of harassment if these acts seriously interfere with the peace and privacy of the victim or cause alarm, distress or harm to the victim ('Coco's Law' Harassment, Harmful Communications and Related Offences Bill 2017)

Prior to the enactment of this Act, perpetrators sharing or publishing intimate images without the subject's consent could not be held criminally liable under Irish law except under limited child protection legislation. The Act also makes it an offence to distribute, publish or send any threatening or grossly offensive communication about or to another person with the intent to cause harm.

In addition to the new offences, the Act extends the scope of harassment under section 10 of the Non-Fatal Offences against the Person Act 1997. Instead of communications 'with' the person, the enactment of this law also covers indirect communications 'about' the victim as well.

This amendment is consistent with the case of DPP *vs* Doherty. To understand this case fully, both the decisions of the Court of Appeal and the Supreme Court of Ireland need to be considered.

In the Court of Appeal, Doherty was convicted on a count of harassment in accordance with Section 10 of the Non-Fatal Offences Against the Person Act 1997 (DPP *vs* Doherty [2019] IECA 209). It should be noted that the Non-Fatal Offences Against the Person Act has been used both in Ireland and the U.K. in reprimanding actions of cyberbullying as harassment and not cyberbullying as a specific offence.

Summarising the facts, the complainant received letters addressed to her about her and leaflets distributed about her. These documents contained derogatory remarks as well as unfounded allegations about the complainant. The case against the appellant was based on circumstantial evidence. Though there was no direct evidence to establish that the appellant was the author and sender of any of the documents that formed part of a campaign of harassment directed at the complainant there was however very strong evidence to suggest that the appellant had sent the email.

The appellant appealed against her conviction on 16 grounds. These were the issues in summary:

Citation Information: Low, W.L, & Gill, D.K. (2022). Malaysia's approach towards cyber bullying: The existing framework. *Journal of Legal, Ethical and Regulatory Issues, 25*(S2), 1-14.

- Retention of data
- Definition of harassment
- Absence of evidence that certain documents were written by the appellant
- Alleged breach of rights to privacy
- Issues arising from presentations by non-expert witnesses
- Refusal to direct the false statement counts
- The closing speech

However none of the grounds of complaint relied upon by the appellant were upheld.

The accused appealed to the Supreme Court of Ireland as the Court of Appeal had dismissed his appeal (DPP *vs* Doherty (2020) IESC 045). The wording and application of Section 10 of the Non-Fatal Offences against the Person Act 1997 was the main issue in the appeal:

Section 10, defines harassment as:

1) Any person who, without lawful authority or reasonable excuse, by any means including by use of the telephone, harasses another by persistently following, watching, pestering, besetting or communicating with him or her, shall be guilty of an offence.
2) For the purposes of this section a person harasses another where
a) He or she, by his or her acts intentionally or recklessly, seriously interferes with the other's peace and privacy or causes alarm, distress or harm to the other, and
b) His or her acts are such that a reasonable person would realize that the acts would seriously interfere with the other's peace and privacy or cause alarm, distress or harm to the other.

Harassment may be "by any means including" a number of activities such as "persistently following, watching, pestering, besetting, or communicating with the victim". The perpetrator must have had the purpose or was aware to some culpable degree, that their actions intended or had a serious risk (recklessness) in causing "alarm, distress or harm" to the victim. The mental element is "such that a reasonable person would realise" that such actions "would seriously interfere with" the victim's "peace and privacy or cause alarm, distress or harm" to them.

The cases of R *vs* ZN (2016) and Lang *vs* Crown Prosecution Service (2017) were cited in interpreting Section 10. In R *vs* ZN, it was clarified that while some conduct may be objectionable or cause alarm, this will not amount to harassment unless the series of actions or communications is also oppressive of the victim. Quoted was a passage from Blackstone's Criminal Practice (2015) at B2.180:

"The practice of stalking is arguably the prime example of harassment…. but a wide range of other actions could, if persisted in, also be so categorised… it must be unacceptable and oppressive conduct such that it should sustain criminal liability."

The case of Director of Public Prosecutions (O'Dowd) *vs* Lynch (2008) was also referred to, where the High Court held that for an action to constitute harassment, persistence is the key element that is required. Though harassment is usually more than one incident, a single count can be deemed as harassment if it is a prolonged, continued action. In this specific case, the behavior in question was also beyond any norm of even poor conduct.

The Supreme Court in Doherty found that indirect communications could constitute harassment and this should be manifestly considered from the victim's perspective. As the appellant here had sent emails to people with close ties to the victim, the court was satisfied that these emails were clearly intended to be received and read by them. This judgment represents a significant development in the law on harassment and confirms that an offensive post or publication which is not shared with the subject of the content namely the victim could still be an offence when the content was clearly intended to be seen by the subject (Fitzgerald, 2020).

Citation Information: Low, W.L, & Gill, D.K. (2022). Malaysia's approach towards cyber bullying: The existing framework. *Journal of Legal, Ethical and Regulatory Issues, 25*(S2), 1-14.

In interpreting section 10(1), these communications do not necessarily require for the victim to be directly addressed (Thomson, 2020) - as long as it was about/intended to be about said victim, and the victim is made aware of it in some way.

The prosecution had initially put forth that the alleged harassment is comparable to "besetting." However, as there were varying opinions by their Lordships on besetting, the conviction of the accused was upheld on the count of harassment instead. The Supreme Court's ruling is significant as it offers an alternative remedy aside from pursuing a defamation action.

Defamation is generally defined as a publication of a false statement that exposes one to hatred, contempt, and ridicule or causes one to be shunned or avoided. Such false statements can amount to libel even where they are an electronic statement in written form. As a result of this, an offensive post and/or publication can be classified as an offence even if it is not directly targeting the victim. Defamation allows for an alternative action for the victim to address the harm they have suffered at the hands of their perpetrator. Indirect social-media posts about the complainant could also fall under the same categorization (Law Society Gazette Ireland, 2020).

RECOMMENDATIONS AND IMPROVEMENTS

Recommendations on a Legal Framework

In defining the scope of cyberbullying behavior having a legal framework coupled with stringent enforcement would help to eliminate and discourage the ongoing increasing instances of cyberbullying in Malaysia.

Any legal response to these issues must take into account the various ways in which cyberbullying offences can take place, the effectiveness of measures to protect victims and prevention of offences as well as data protection (Adediran, 2020). Considering Singapore's approach, there are different alternative measures both civil and criminal depending on the gravity of each case and the relevant offences which include unlawful stalking and doxing.

Whilst Ireland has recently enacted their own law that targets cyberbullying and online abuse, the UK continues to rely on their existing legislations on harassment to deal with offences of harassment and cyberbullying.

Would the answer lie in having a more targeted approach? One of the main issues that continue to persist is the broad spectrum of what "cyberbullying" amounts to. To effectively answer this question extensive research is needed to determine what type of behavior is socially acceptable and that which is unacceptable, this is needed before laws can be enacted to curb or criminalize cyberbullying.

A study and analysis that compared cyberbullying measures of the UAE, US, UK and Canada suggested several factors (Hosani et al., 2019) to consider in implementing any given framework including:

- Defining the methodology and research questions for a comparative study
- Understanding the cultural and religious differences of each country before choosing the legal systems to be compared
- Understanding how the laws of each country are applied in resolving international cases

Currently in Malaysia, research on anti-cyberbullying laws is still being conducted. Within any legislative framework social responses which may help to support victims and to bring about improvement should also be considered. In an op-ed by Kasthuri Patto, Batu Kawan MP and International Secretary for the Democratic Action Party Women (Patto, 2020), he wrote on the need and urgency to set up a Parliamentary Select Committee or for an All-Party Parliamentary Group to address cyberbullying and to work on an overall collective opinion pool.

Citation Information: Low, W.L, & Gill, D.K. (2022). Malaysia's approach towards cyber bullying: The existing framework. *Journal of Legal, Ethical and Regulatory Issues, 25*(S2), 1-14.

Other Improvements

Aside from the implementation of a legal framework, other methods can work hand-in-hand to combat the prevalence of cyberbullying within the community.

In 1999, Professor Lessig at Harvard Law School suggested that online behaviors could be monitored in other ways besides implementing laws. This includes regulating social norms, existing laws and the computer coding (Lessig, 2020). How should online behavior be monitored taking into account rights of privacy? The law should remind the perpetrators that there are consequences to their actions. Social norms keep people in check in identifying inappropriate behaviour online. A combination of coding, software and online protocols help to "constrain" behavior by making certain behavior possible or not. These can take the form of choices for passwords, tracing and the choice to opt-in or opt-out.

Lessig's suggestion was based on the premise that the law may not be able to keep up with technology that is ever-changing and developing. An accessible starting point could involve addressing the lack of clear rules in respect of appropriate online social behaviour. If the rules of acceptable conduct and consequences are defined clearly, and enforced by internet service providers, that accountability may encourage more civil interactions online (Harrison, 2015). Online interactions may be more civil if there is a defined social norm for what is considered appropriate conduct.

Enforcement

Considering both policy and practice, a majority of cyberbullying cases either go unreported or rarely involve the response of law enforcement. However, the police and officers of the law should also use their discretion in handling the situation in a way that is appropriate given the nature of the circumstances and offences involved (Patchin et al., 2020). Confronting a first-time offender in comparison to a repeated offender would involve the need for different approaches. Factors taken into account would include how the case is discovered, investigated, how much harm has occurred, what evidence is available, who is involved and how well-trained the officers are in responding to such complains. The impact, both physical and emotional suffered by the victim should be considered. The sensitivity of investigating officers involved will have an impact on whether cyberbullying victims will speak out about what they are going through.

Social Support

A study conducted among Vietnamese university students sought to determine whether social support mediates the relationship between cyberbullying victimization and depressive symptoms in university students. 606 students participated in questionnaires related to their experience of being a cyberbullying victim, most demonstrated depressive symptoms and the perceived need for social support.

It was discovered that social support partially mediates the relationship between victims of cyberbullying and depressive symptoms. Parental support, peer support and special persons support does play an important role in helping cyberbullying victims. Social support is considered as an essential protective factor for adolescents when they are placed in such situations (Ho, 2020).

Education

The importance of public awareness and education should also be emphasized on.

In South Korea, legislators campaigned for a cyberbullying bill as well as making cyberbullying education compulsory in schools and private businesses. These were brought

Citation Information: Low, W.L, & Gill, D.K. (2022). Malaysia's approach towards cyber bullying: The existing framework. *Journal of Legal, Ethical and Regulatory Issues, 25*(S2), 1-14.

into discussion following the death of two young K-pop stars who had faced online abuse (Sunday Telegraph, 2019).

In cases involving minors their limited cognitive, emotional and social capacity as well as their anonymity are factors that need to be considered as well. This is not to say that they should be relieved of their responsibility were minors are involved in cyberbullying but rather the law and its enforcers have to be creative in dealing with all forms of perpetrators regardless of their age and status. Instead of civil liability, supervising and responding to their conduct may be a more appropriate alternative (Ronen, 2020).

Education in schools or a community-based approach might also be an effective method in dealing with cyberbullying. According to a comparative study (Purdy, N., & Mc Guckin, 2015) that was conducted in Northern Ireland and the Republic of Ireland less than half of the school leaders felt confident in their knowledge of the legislation surrounding cyberbullying. A large majority of them also touched on the importance of professional development courses, more practical guidance and more resources to help schools respond to cyberbullying.

In a study published in the Canadian Journal of Behavioural Science, it was discovered that the participants were mainly unaware of existing cyberbullying laws with differing opinions on what constitutes cyberbullying and actions that should be recognized as online illegal behavior. This study supports the notion of developing a more concrete definition of cyberbullying as this will also ensure consistency across legal responses in such cases (Patterson, 2015). Hence, there is a need for both prevention and punitive measures for these behaviors to be clearly defined (Foody, 2017).

CONCLUSION

In conclusion within Malaysia although there are no specific laws on cyberbullying , there do exist a bundle of rights within various Acts that can be thought of providing a rough de facto basis for protecting victims of online abuse however there is nothing specific that defines and adequately deals with cyberbullying offences. Accordingly research and consultation is needed to look into specific legislation to deal with cyberbullying offences in line with some of the laws and responses considered by other common law jurisdictions such as Singapore the United Kingdom and Ireland.

This showcases the primary argument that there remains a gap in the law in Malaysia on cyberbullying which needs to be addressed and the proper forum lies within Parliament to consider and introduce specific legislation to prevent abuse and intrusions that expose victims to cyberbullying rather than a rough de facto basis of laws which fail to address the offences specific to online abuse.

Aside from a legal framework public awareness, education and social norms on what type of online behavior is acceptable along with community efforts and support are needed to effectively combat the prevalence of cyberbullying in Malaysia.

REFERENCES

Director of Public Prosecutions (O'Dowd) *vs* Lynch. (2008). IEHC 183, [2010] 3 IR 434.
Director of Public Prosecutions *vs* Doherty. (2019). IECA 209.
Director of Public Prosecutions *vs* Doherty. (2020). IESC 045.
Kellett *vs* DPP. (2001). EWHC Admin 107.
Lang v Crown Prosecution Service. (2017). EWHC 339 (Admin)
R *vs* ZN. (2016). EWCA Crim 92.
R *vs* Debnath. (2005). EWCA Crim 3472.
Adediran, A.O. (2020). Cyberbullying in Nigeria: Examining the adequacy of legal responses. *International Journal for the Semiotics of Law*.

Citation Information: Low, W.L, & Gill, D.K. (2022). Malaysia's approach towards cyber bullying: The existing framework. *Journal of Legal, Ethical and Regulatory Issues, 25*(S2), 1-14.

Ayub, Z., Yusoff, Z., & Haq. M. (2020). Legal framework on protection of children against cyberbully in Malaysia: A cause of great concern. School of Law, Universiti Utara Malaysia. *International Journal of Advanced Science and Technology, 29*, 8, 143-154.

Abdullah, T. (2020). 'We must draw the line with cyberbullying' (New Straits Times, 5 June 2020).

Alkhatib, S. (2021). 'Teen who threatened EPL player, family gets probation' (The Straits Times, 8 July 2021).

Bernama. (2020). 'Strong calls for cyberbullying to be categorized as criminal offence – Saifuddin' (Astro Awani, 9 Dec 2020).

Basyir, M., & Perimbanayagam, K. 'Cyberbullying victim found dead after viral Tik Tok video'. (2020).

Coco's Law - Harassment, Harmful Communications and Related Offences Bill 2017.

Criminal Law Review. (2006). 'Sentencing: harassment' Crim. L.R, 451-453.

Dunphy, L. (2021).'Coco's Law: 'Long after we're gone, her name will still be there'' (Irish Examiner, 13 February 2021).

El Asam, A., & Samara, M. (n.d.). 'Cyberbullying and the law: A review of psychological and legal challenges' [Book Section] Computers in Human Behavior. - [s.l.]: Department of Psychology Kingston University London Penrhyn Road Kingston upon Thames KT1 2EE UK.

Edwards, A. (2010). 'Criminal law – extending the jurisdiction of the magistrates' courts' (Law Society Gazette, 14 Jan 2010) (Online edition).

Foody, M., Samara, M., El Asam, A., Morsi, H., & Khattab, A. (2017). 'A review of cyberbullying legislation in Qatar: Considerations for policy makers and educators'. *International Journal of Law and Psychiatry, 50*, 45-51.

Fullerton, J. (2019). 'Teenage girl kills herself 'after Instagram poll' in Malaysia.' (The Guardian, 15 May 2019).

Fitzgerald, M., & Kehoe, S. (2020). 'Supreme Court Expands Scope of Harassment to Offensive Online Posts'. (2020).

Hosani, H.A., Yousef, M., Shouq, S.A., Iqbal, F., & Mouheb, D. (2019). "A Comparative Analysis of Cyberbullying and Cyberstalking Laws in the UAE, US, UK and Canada," 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), 1-7.

Harrison, T. (2015). 'Virtuous reality: Moral theory and research into Cyber-Bullying'. *Ethics and Information Technology, 17*(4),275–283.

Ijachi, O. (2019). 'Social Media Access and Cyberbullying—A Nigerian Perspective'. *International Journal of Innovative Studies in Medical Sciences, 3*(3), 5–9.

Kipper, B., & Ramey, B. (2020). 'No bullies, how to save our children from the new American bully' (Morgan James Publishing, 2020).

Law Society Gazette Ireland. (2020). 'Wider harassment recourse after Supreme Court ruling' (Law Society Gazette Ireland, 7 September 2020).

Lessig, L. (1999). 'The law of the horse: What Cyberlaw Might Teach'. *Harvard Law Review 113*, 2, 501–549.

Malay Mail, 'Communications Ministry preparing Cabinet paper on anti-cyberbullying laws'. (2021).

Mirror, 'Coco's Law signed in memory of bullied girl'. (2020).

Myers, C., & Cowie, H. (2019). 'Cyber bullying across the lifespan of education: Issues and Interventions from School to University'. *International Journal of Environmental Research and Public Health, 16*(7), 1217.

Nazari, T. (2020). 'Malaysia Might Make Cyber bullying Illegal Soon, But Are We Ready?' (The Rakyat Post, 9 Dec 2020).

Nur, A. (2020). 'Malaysia surpasses 26 countries to become 2nd in Asia … cyber-bullying' (The Sun Daily, 20 July 2020).

Newall, M. (2018). 'Cyberbullying: A Global Advisor Survey' Ipsos Public Affairs' (Ipsos, 2018).

Pannick, L., & Herberg. (n.d.). Human rights law and practice (*2nd Edition*), 363.

Patto, K. (2020). MP SPEAKS | There's a great need for cyberbullying law. (Malaysiakini, 20 September 2020).

Patchin, J.W., Schafer, J., & Jarvis, J.P., 'Law enforcement perceptions of cyberbullying: Evolving perspectives' (2020) *Policing, 43*(1), 137-150.

Patterson, V.C., Closson, L.M., & Patry, M.W. (2019). 'Legislation awareness, cyberbullying behaviours, and cyber-roles in emerging adults'. *Canadian Journal of Behavioural Science / Revue Canadienne Des Sciences Du Comportement, 51*(1), 12–26.

Penal Code (Act 574), 44.

Purdy, N., & Mc Guckin, C. (2015). Cyberbullying, schools and the law: A comparative study in Northern Ireland and the Republic of Ireland, *Educational Research, 57*, 4, 420 – 436.

Ronen, P. (2020). 'Civil liability for cyberbullying', *Uc Irvine Law Review, 10*(4), 1219–1219.

Selangor Journal, 'MCMC addresses over 11,000 complaints within first six months this year' (Selangor Journal, 12 August 2020).

Singapore Legal Advice (2021). 'Applying for a Protection Order for Harassment in Singapore' (Singapore Legal Advice, 9 June 2021).

Sunday Telegraph. (2019). 'K-pop star's law will tackle cyberbullying' (Sunday Telegraph, 1 December 2019).

The Star Online. (2019). 'Global debate over girl's death' (The Star Online, 17 May 2019).

Citation Information: Low, W.L, & Gill, D.K. (2022). Malaysia's approach towards cyber bullying: The existing framework. *Journal of Legal, Ethical and Regulatory Issues, 25*(S2), 1-14.

The Star Online. (2020). 'Minister: MMU to study need for anti-cyberbullying laws' (The Star Online, 4 July 2020).
The Sun Daily. (2020). 'Strong calls for cyberbullying to be categorized as criminal offence – Saifuddin' (The Sun Daily, 8 December 2020).
Quynh Ho, T., Li, C., & Gu, C. (2020). 'Cyberbullying victimization and depressive symptoms in Vietnamese university students: Examining social support as a mediator'. *International Journal of Law, Crime and Justice*, *63*, 100422.
Thomson Reuters. (2020). 'Discussion on harassment based on (The People (DPP) *vs* Doherty (2020) IESC 45' (Thomson Reuters, 2020) Criminal Law Week, *46*, 10.
Tithe an Oireachtais Houses of the Oireachtas. (2020, 28 Dec). Harassment, harmful communications and related offences act 2020.
Vin, A.M. (2019). 'Ministry of health: You Can Be Fined RM50K Or Jailed For Calling Someone Fat Online'. (2019).
Walker, A. (2009). 'Cyber bullying: Bullying in the digital age' – By Robin M. Kowalski, Susan P. Limber and Patricia W. Agatston. *Support for Learning, 24*, 207-207.
Wira, B. (2019). '3 in 10 young people in Malaysia cyber-bullied' (#children4change, 2019).
Wenjun, P. (2019). 'The Effect of Section 114A of the Evidence Act 1950 on Internet Publications' (Thomas Philip Advocates & Solicitors, 16 April 2019).
Wong, L. (2019). 'Have You Been Cyberbullied in Singapore? The law can help' (Singapore Legal Advice, 24 October 2019).
Xia, L. (2020). 'Joining up to fight cyberbullying' (The Star Online, 1 April 2020).
Yeoh, A. (2020). 'MCMC: 48 court charges filed over misuse of social media, including child porn' (The Star Online, 11 November 2020).

Received: 11-Dec-2021, Manuscript No. JLERI-21-8209; **Editor assigned**: 13-Dec-2021, PreQC No. JLERI-21-8209(PQ); **Reviewed:** 21-Dec-2021, QC No. JLERI-21-8209; **Revised:** 29-Dec-2021, Manuscript No. JLERI-21-8209(R); **Published:** 11-Jan-2022

Citation Information: Low, W.L, & Gill, D.K. (2022). Malaysia's approach towards cyber bullying: The existing framework. *Journal of Legal, Ethical and Regulatory Issues, 25*(S2), 1-14.