12-7-2022

Cyberbullying Prevention and Reduction Strategies: An Exploratory Study.

Chintha Kaluarachchi
RMIT University, c.kaluarachchi@deakin.edu.au

Van-Hau Trieu
Deakin University, t.trieu@deakin.edu.au

Cyberbullying Prevention and Reduction Strategies: An Exploratory Study.

Full Research Paper

Chintha Kaluarachchi
Centre for Cyber Security Research and Innovation (CCSRI)
RMIT University
Melbourne, Victoria, Australia.
Email: S3863295@student.rmit.edu.au

Van-Hau Trieu
Deakin Business School
Deakin University
Burwood, Victoria, Australia.
Email: t.trieu@deakin.edu.au

Abstract

Cyberbullying was described as a complex phenomenon by the court and other legal practitioners involved in court cases. While previous research has significantly added to our understanding, there has been far less information systems research conducted in relation to the prevention and reduction strategies to combat cyberbullying. It is essential to focus on the primary entities of cyberbullying and technology usage to combat cyberbullying. Therein, we observed the salient entities of the 'victim,' 'offender,' and their technology use regarding cyberbullying. The study aims to gain a better understanding of cyberbullying and identify strategies to minimize and prevent this growing societal problem. Our study findings show that it is crucial for victims to understand how to use digital tools, platforms, and social media responsibly. From the standpoint of the offender, they must comprehend their obligations as digital citizens and cyber-ethics to change their immoral actions to prevent deviant behaviours like cyberbullying.

Keywords: Cyberbullying, Cyber-ethics, Responsible use of IT, Social media, Internet

1 Introduction

Jessica Logan, 18 years old, a former high school student at Sycamore High School, attempted suicide by hanging on July 3, 2008. Her death has been attributed to the online distribution of a naked photo of her and online harassment. Jessica was continually harassed by her boyfriend Ryan Salyers and other students at Sycamore High School by maliciously circulating a nude photo of her online. Jessica tried to end the harassment at school and seek help from the relevant authorities and school staff. She did not get their help and failed to stop the harassment, which escalated to the point that deprived Jessica of her access to education and caused severe emotional distress, eventually leading Jessica to commit suicide

(Retrieved from: Case No. 1:09-cv-885).

Stories like Jessica's are becoming increasingly common and involve persons who committed suicide because of "cyberbullying" in many nations (Kowalski et al. 2008). Cyberbullying has emerged as a new form of bullying and has been defined as "*an intentional harmful behaviour carried out by a group or individuals, repeated over time, using modern digital technology to aggress against a victim who is unable to defend him/herself*" (Campbell and Bauman 2018, p.3). The rapid advancement of technology gives cyberbullies many opportunities to act cruelly and harm others online, yet it also makes it possible for them to go unnoticed due to the anonymity facilitated by these online platforms. Cyberbullying thrives on social media platforms and mobile devices, although similar behaviours happen in a variety of online venues (Kowalski et al. 2014). According to the Australian eSafety Commissioner, cyberbullying can also occur through online chat and messaging services, text messages, emails, message boards, and online forums (eSafety Commissioner 2020) that threaten, harass, embarrass, or socially exclude peers (Hinduja and Patchin 2009; Williams and Guerra 2007). Moreover, cyberbullying can happen anywhere and anytime online, in contrast with traditional bullying (Kowalski et al. 2019) which makes cyberbullying more pervasive and harmful than traditional bullying (Huang et al. 2018b).

According to a recent literature review, the percentage of cyber victims in the general population could be as high as 90.86%, while the percentage of cyber perpetrators could be as high as 54% (Jenaro et al. 2018). Pew Research Centre study shows that four out of ten adults in the United States have experienced online harassment or abusive behaviours. Among those who have been harassed online, 18% have been subjected to severe online abusive behaviours such as physical threats and/or sexual harassment (Pew Research Center 2017). While the general prevalence of this sort of abuse has remained unchanged since 2017, there is evidence that online harassment has intensified (Wang 2022) since then. As a result, cyberbullying has gotten much attention around the world, with many OECD countries leading the way with their own e-safety commissions (OECD 2020). Furthermore, scholars are increasingly pushing for a more complete understanding of cyberbullying as a rising societal phenomenon (Chan et al. 2019) to develop laws, regulations, and technological solutions to combat it. However, most of the research on cyberbullying has concentrated on the prevalence and predictors of cyberbullying (Lee et al. 2017), the comparison of cyberbullying and traditional bullying (Hinduja and Patchin 2010), coping mechanisms for dealing with cyberbullying (Raskauskas and Huynh 2015), the characteristics of cyberbullying offenders, victims, and bystanders (Lund and Ross 2017), as well as risk and protective factors for cyberbullying (Chen et al. 2017; Guo 2016).

Previous research on cyberbullying has significantly added to our understanding, there has been far less information systems research conducted in relation to the prevention and reduction strategies that combat cyberbullying. Specifically, prior studies did not focus on investigating digital programs or strategies that can help educate and assist people in countering cyberbullying (Kowalski et al. 2008; Sabella et al. 2013). Therefore, this paper aims to gain a better understanding of cyberbullying and identify strategies to minimize and prevent this growing societal problem. Against these objectives, we ask: *What preventive and reduction strategies can be used to combat cyberbullying?*

2 Background

2.1 Cyberbullying

Cyberbullying is defined as *"an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and overtime against a victim who cannot easily defend him or herself"* (Smith et al. 2008, p. 376). The terminology used in cyberbullying research is derived from traditional bullying literature (Chan et al. 2021). Many past researchers considered cyberbullying as an

extension of traditional bullying in which intention, aggressiveness, power imbalance, and repetition are core features of this phenomenon (Alipan et al. 2020). However, cyberbullying is more pervasive than traditional bullying (Huang et al. 2018a) and can occur regardless of time or place. Cyberbullying can occur through a variety of online formats, including instant messages, emails, and blogs, and is particularly prevalent on social media platforms and mobile devices (Kowalski et al. 2014). Previous research has shown that social networking sites account for 70% of cyberbullying, followed by emails (49%), instant messages (50%), and mobile phones (44%) (Kowalski et al. 2017).

Cyberbullying has become more prevalent because of the rapid development of digital technologies that enable connected societies and social media platforms, as well as the widespread use of mobile devices (Kaluarachchi et al. 2020). In addition, the anonymity of online communication frees people from social and normative restraints on behaviour, which increases the likelihood of aggressive and improper behaviour in cyberspace (Moore et al. 2012). Additionally, stressful life events like the end of a love relationship, employment stress, or other problems cause negative emotions like anger, frustration, or grief that may cause people to act out or engage in other undesirable behaviours such as cyberbullying as a way to cope (Agnew 2014).

Numerous studies have found a connection between cyberbullying and psychological and physical harm, including depression (Perren et al. 2010), distress (Perren et al. 2010), anxiety (Kowalski et al. 2014), increased psychosomatic symptoms (Sourander et al. 2010), intrusive thoughts of self-harm and suicide ideation (Kowalski et al. 2014).

2.2 Cyberbullying as an unethical and deviant behaviour

Cyber risks and harms, including cyberbullying, are increasingly occurring in people's daily lives (Cocking and Van den Hoven 2018). The Australian Human Rights Commissioner Branson (2011) highlighted that *"cyberbullying is a growing problem confronting the nation with the potential for serious mental and physical impacts. This is a human rights issue which could affect a young person's right to education, health, and the right to be free from violence and harassment whether at home, school, work or anywhere else."*

Cyberbullying is fostered by the emergence and usage of communication devices such as smartphones, tablets, and smartwatches (Chan et al. 2019; Lowry et al. 2016) that can convey messages containing emotion and human elements (Burton-Jones et al. 2017). Technological and social changes create new opportunities for unethical and deviant behaviour (Felson and Clarke 1998). Therefore, shifting social activities from an offline to an online environment provides more opportunities for offenders to engage in cyberbullying as they can easily find vulnerable victims by browsing their online profiles (Chan et al. 2019). The cyber environment with easy access to various communication personal devices produces an opportunity for bad-tempered people to release their negative emotions by bullying vulnerable victims and publicizing humiliating information (Zhang et al. 2021)

Cyberbullying can negatively impact someone's safety, sense of self, health, and educational rights (Elci and Seckin 2016) as well as violate their way of life and feeling of well-being (So and Lenarcic 2015). Therefore, cyberbullying is viewed as unethical and deviant behaviour (Harrison 2022), which usually causes people to feel concerned, alarmed, afraid, or frustrated. Specifically, cyberbullying can make the victims feel threatened in many ways by strangers disseminating rumours, posting humiliating images, revealing, or stealing personal information, and sending threatening or offensive messages. This causes a great deal of distress and disruption in people's lives (Kaluarachchi et al. 2020; Perren et al. 2012). Cyberspace has provided weapons for cyberbullying (Harmon, 2004) and has become a real issue without rules within civilised society (Shariff and Hoff 2007). Therefore, cyberbullying can be identified as a digital ethics concern.

3 Research Methodology

To address our research question, we use notable court case transcripts in relation to cyberbullying cases as publicly available data is a rich source of knowledge for information systems research (Ghazawneh and Henfridsson 2013). We used cyberbullying court cases from 2008- 2020 and extensive quotes from the selected court case transcripts, which took place between the relevant practitioners such as lawyers, judges, police officers, psychologists, and other technical specialists.

First, the study searched legal databases (e.g., AustLII, CanLII, WorldLII, and JUSTIA US Law) using keywords or related terms of cyberbullying, cyber harassment, and cyberstalking. The cases that appeared in the search results were downloaded and saved individually. The researchers next skim-read these cases to ascertain their basic content. All selected cases from the skim reading were examined in

detail to identify whether the case is related to 'cyberbullying' and adults. Cases were excluded from the final sample if the case refers to incidental case law unrelated to the circumstances of cyberbullying among adults and if neither the reasons nor the circumstances of the cyberbullying were considered. Our search identified 20 court case transcripts, each approximately 50 pages long. The small sample size is justified using Patton, who argued that *"the validity, meaningfulness, and insights generated from qualitative inquiry have more to do with the information-richness of the cases selected and the analytical capabilities of the researcher than with sample size"* (Patton 2002, p. 185). Then we inductively derived codes in relation to our research question "strategies to prevent cyberbullying" to combat this immerging societal issue.

Bandara et al (2015) specified three approaches that are central to qualitative content analysis: inductive category development, deductive category application, and mixed approach. As a result, the court case data in our study were analysed in an inductive way given that this important domain of analysis is often absent by detailed theoretical and practical considerations. Following Bandara et al. (2015) suggestions, NVivo© was used as a support tool during the coding process (Bandara et al. 2015). We used "In-vivo coding" to code selected court cases inductively. In-vivo coding is a technique of *"Assessing a label to a section of data, such as an interview transcript, using a word or short phrase taken from that selection of the data"* (King, 2008, p.3). We should note that no themes or subthemes were used at this exploratory stage as we let data talk (Rinta-Kahila et al. 2021). All in-vivo codes were then grouped under pre-defined themes. Two coders were involved in the coding process to ensure the validity and reliability of the data. Table 1 below summarizes the details related to the court cases used in this study.

Case # and Reference	**Behaviour**	**Online tools**	**Case # and Reference**	**Behaviour**	**Online tools**
Case #1 [2016] SASC 135	The appellant sent private Facebook messages to the victim and made humiliating public posts about the victim on Facebook.	Facebook	Case #11 2018 ONSC 4726	The offender and the victim had on, and off an intimate relationship and after some time they stopped their relationship. Then the offender created a fake Facebook profile and uploaded five intimate images of the victim without her consent to humiliate her.	Facebook
Case #2 [2017] QCA 307	Using a carriage service to transmit and publish child pornography material; make a threat to kill; and menace, harass or offend victims.	Mobile chatting app/ Facebook / calls	Case #12 A-4787-11T1	The offender had used a webcam to video stream the victim's private sexual encounter with another man, invasion of privacy, and intimidation.	Webcam / Twitter
Case #3 2015 NSSC 71	"Progression of online abuse" against the victim by way of text messages, email, and public Facebook posts.	Facebook / Emails	Case #13 [2013] FMCAfam 284	The father and his family had posted denigrating messages on Facebook about the mother.	Facebook
Case #4 2014 MBPC 63	A relentless campaign of cyberbullying and sexual exploitation of a 14-year-old girl.	Facebook / Other social media networks	Case #14 2016 BCSC 686	The offender made posts on Facebook targeting a local schoolteacher. These posts then "went viral", with many of the offender's friends responding to the posts with more defamatory remarks.	Facebook
Case #5 2016 BCPC 400	The offender took pictures of his former girlfriend's bare breasts on his phone and transmitted them to two of his friends.	Mobile text messages	Case #15 [2014] VSCA 323	The offender used a carriage service to solicit child pornography materials, and use a carriage service to transmit indecent communication to a	Facebook

				person under 16 years of age. This matter involved three child victims who were aged between 14 and 15 years old and were known to the offender.	
Case #6 [2013] WASCA 243	Engaged in sexual activity with girls under the age of 13-16 years using the Internet and menacing, harassing, or offensive toward them	Facebook / Skype/ YouTube	Case #16 774 S.E.2d 337 (N.C. Ct. App. 2015)	The victim's classmates began posting negative comments and pictures of him on his Facebook page.	Facebook
Case #7 [2021] NSWDC 218	The offender engaged in a series of online conversations with and transmitted indecent materials to an Assumed Online Identity (AOI) a fictitious 14-year-old female child used by police.	Kik, WhatsApp	Case #17 CR 08–0582–GW	Offenders set up a profile for a fictitious 16-year-old male juvenile named "Josh Evans" on the website ("MySpace"), to flirt and humiliate the victim.	My Space
Case #8 2016 ONCJ 547	The offender posted nude and semi-nude images of his underage girlfriend to a public pornographic website without her consent.	Pornographic Website	Case #18 922 N.W.2d 886 (Mich. Ct. App. 2018)	The offender repeatedly posted comments about his former attorney on his Facebook, and in the comments sections of online news articles.	Online news articles/ Emails/ Facebook
Case #9 2019 NSSC 370	The victim's ex-husband and his new girlfriend created Facebook posts to cyberbully the victim.	Facebook	Case #19 RWT 11-091	The offender posted threats and other potentially emotionally distressing speech aimed at a public figure, a religious leader using Twitter and his blog site.	Twitter, Other Internet Websites, Blogs
Case #10 [2011] QCA 132	The offender posted several offensive pictures and comments on the Facebook tribute pages to several dead or missing children.	Facebook tribute pages	Case #20 [2014] QCA 353	The offender was involved in sexual activities with young girls aged 13 and 14 via the internet using webcams. He further recorded the incident and cyberbullied them.	MSN Messenger Vampire Freaks" My Space Emails

Table 1: Court Case Details

4 Courts Case Findings: Strategies to Combat Cyberbullying

An important aspect of preventing cyberbullying is the responsible use of technology, which refers to understanding the appropriate and inappropriate uses of technology in cyberspace (Kaluarachchi et al. 2020). Without taking ethics and governance into account when using technology, undesirable results like cyberbullying may occur and have an impact on society. Therefore, we investigate how to prevent deviant online behaviours such as cyberbullying and identify important prevention and reduction strategies that can be used to combat cyberbullying in relation to both victims and offenders of cyberbullying. In terms of the victims, it is particularly important that they have a good understanding of the responsible use of technology tools and platforms. From the offender's perspective, they need to understand digital citizenship responsibilities as well as cyber-ethics to change their immoral behaviours.

4.1 Awareness Raising

Some of the investigated court cases indicate that the 'victim's reckless and irresponsible usage of ICT' is one of the main reasons why someone becomes the target of cyberbullying. For instance, in case #8 the victim on request of her former boyfriend *"took photos of herself and posted them on a private internet site that only the two of them could access."* Case #11 is another notable example of the victim's irresponsible use of ICT. Case files show that *"Ms. T. recognized the origin of the relevant intimate images of her, posted to the fake Facebook account, as they had been taken by Mr. B., with Ms. T.'s*

knowledge and consent, using Mr. B.'s personal cellular phone, during a previous date that took place during their intimate relationship. These victims shared these nude pictures with their former partners with the reasonable expectation that they would keep them private and not show them to anybody else. However, they betrayed their confidence and made use of these private photos for cyberbullying due to dysfunctional relationships. These instances show how the victims of these cyberbullying incidents ended up there because of their own irresponsible usage of ICT.

Another significant reason is the victim's lack of technical knowledge and skills for detecting fraudulent activities in cyberspace. Some of the offenders can manipulate or deceive vulnerable people into sharing something personal, or intimate photos, which they subsequently use as a weapon in cyberbullying. For example, Case #2 shows that *"After persistent requests, AB provided a photograph of her naked breasts to Hannah's account. That photograph was then used as a means of blackmailing her"*. Case #19 shows that *"Feeling that she had no other choice this complainer sent three photographs of her naked breasts to the respondent."* Most of these victims succumbed to the threats of the offenders due to their lack of technological skills and abilities to recognize fraudulent activities in cyberspace.

To safeguard these vulnerable people against undesired encounters, and gain responsible behaviours in cyberspace, it is essential to raise awareness, and develop skills, capabilities, and netiquettes for people to manage cyberbullying risks and harms. Past researchers also asserted that awareness-raising and professional development programs would guide online users, in navigating the problems of cyberbullying (Slonje et al. 2013; Spears et al. 2014). This has been acknowledged in most of the court cases which we analyzed. Case #1 reported that the number of suicides in Australia that have been linked to cyberbullying is on the rise and the importance of raising public awareness of this potentially fatal online behaviour.

Furthermore, people spend a lot of time on social media today, oblivious to its effects on their daily lives. Social media literacy is an emergent idea that has not been fully explored in the literature, but it is pertinent in this situation (Polanco-Levicán and Salvo-Garrido 2022). Because vulnerable and disadvantaged people may be less likely to understand the complexity of the systems they are using (United Nations Children's Fund 2017). Therefore, it is necessary to have social media literacy programs to educate these vulnerable people. Facebook's "Digital Literacy Library" also offers lesson plans created especially for young people to help them advance their knowledge of security, positive behaviour, privacy, and community involvement modules (Facebook 2020b). The importance of social media literacy is also mentioned in the number of court cases we analyzed.

4.2 Safe Use of the Internet, Social -Media Platforms, and Other Tech Tools

The advent of the Internet with 24-hour connectivity and social networking sites creates new opportunities for cyberbullying and is echoed in all cases (100%) as mentioned in previous studies (Chen et al. 2017; Kowalski et al. 2019; Lianos and McGrath 2018). People can be a target of cyberbullying via the latest games, apps, instant message apps, and social media (eSafety Commissioner 2020). However, technology can also shield people from cyberbullying. Therefore, we tried to investigate the most effective technical remedies that can be used to safeguard people from cyberbullying.

These technological remedies may include blocking undesirable users, anonymous messages, changing their usernames and passwords, or deleting accounts (email, social media) associated with cyberbullying (Smith et al., 2008). Blocking messages/identities was mentioned as the most effective way to stop cyberbullying in Smith et al.'s focus group session (Smith et al. 2008). This was also discovered to be the most preferred method in court case analysis. For instance, in Case#1, *"MH then blocked the appellant as a Facebook friend*" to stop sending him private Facebook messages by the offender. Again Case #9 shows that the offender *"was blocked from their Facebook friend list, and the postings were "private"*.

Avoidance and confrontation are also effective methods for stopping cyberbullying (Hoff and Mitchell 2009). Therefore, some victims disabled or deleted their accounts permanently to avoid further cyberbullying. Case #20 shows that the offender *"tried to get in contact with her a week or two after the video recording, but she deleted her email account"* to prevent further communication with the offender. Case #11 also revealed that *"the relevant Facebook profile containing the intimate images was removed from the internet "within hours" of Ms. T. learning about it"* to prevent further distribution of her intimate images. Also, users can adjust their privacy settings in their social media profiles to avoid unnecessary communications. The importance of this is also mentioned in court cases. In case #18, the victim *"Buchanan immediately adjusted her Facebook privacy settings to prevent Crisler from tagging her in the future."* All these cases demonstrated the effectiveness of these technological remedies in cutting off contact with the offenders and stopping further cyberbullying.

An automated social media platform that is globally and freely accessible to your Facebook friends, their friends, and others and has become a ubiquitous technology platform for cyberbullying (Livingstone et al. 2011). Case #13 has shown that *"while social media can be used for good, often it is used as a weapon, either by one or both of the parties and or by their respective supporters."* Most of the cases investigated showed how social media platforms helped spread false information about the victims on Facebook to engage in cyberbullying. However, using social networking sites responsibly would allow users to use their benefits while reducing their exposure as a prime target for online deviant behaviours. Users should share the least amount of personal information possible, especially on social networking sites, safeguard their identity, and report any incidents to the appropriate authorities (Coventry et al. 2014). Case # 9 also confirmed that *"Facebook is not used as a means by which account holders carry on monologues with themselves; it is a device by which users share with others information about who they are, what they like, what they do, and where they go, in varying degrees of detail. Facebook profiles are not designed to function as diaries; they enable users to construct personal networks or communities of "friends" with whom they can share information about themselves, and on which "friends" can post information about the user.*"

Moreover, we can see that social media organizations are taking more proactive measures to combat cyberbullying on their platforms. Their "Help Centers" offers safety and security tools to deal with online abuse and bullying to support its members. Information on privacy controls can be found in the Help Center, including "How to secure personal information", and "How to deal with spam, fraudulent accounts, and sensitive content". Furthermore, the Facebook Help Centre consists of a series of information sources related to bullying including "what should they do if being bullied, harassed or attacked by someone on Facebook", "how to remove users from abusive tags", "unfriending and blocking Facebook users" (Facebook 2020a; Twitter 2019). The importance of these tools has been discussed in court cases as well. Case #19 acknowledged this *"Twitter provides detailed instructions for blocking Tweets from another user as well as for "unfollowing" another user, i.e., blocking Tweets from a user that one used to follow."* Moreover, most social media platforms comprise a reporting feature that allows users to report abusive content on their platforms, then they take it down. Case #2 shows that the victim *"AB's reporting it to Facebook, the material was removed within about a quarter of an hour."* Case #11 also shows that upon the victim's request, *"Steps were taken to "take down" the fake Facebook site "very quickly."* This is usually the quickest method of getting the harmful content removed. These social media tools were effective in preventing a vulnerable person from becoming a cyber victim.

4.3 Digital Citizenship and Cyber-ethics

Crime, deviant, and immoral behaviors are more common among the mentally ill or those suffering from alcohol or drug addiction, as well as other mental disorders, such as personality disorders (Håkansson and Berglund 2012). Approximately 20% of court cases revealed that the perpetrators had depression, anxiety, and deficits in their psychological functioning. For example, in case #2, the psychologist who assessed the offender's psychological functioning determined that: *"The applicant showed signs of a persistent depressive disorder. The applicant's level of intelligence is in the low average to average range."* In addition, in case #6, the offender's immoral behaviour arose due to his/her psychological distress. The perpetrator's emotional state was revealed to be *"High anxiety, moderately high stress, and severe depressive symptoms" (Case#6).* Those deficits in their psychological functioning reduce their power or ability to control their emotions, behavior, or actions and remove the normal inhibitions that prevent most individuals from engaging in deviant behaviors.

Additionally, the presence of technology-enabled anonymity encourages the phenomena of online disinhibition. It frees people from the constraints of acceptable behaviour in society, which leads to an increase in violence and improper behaviour online (Moore et al. 2012). Case #15, the court shows that *"Unlike traditional bullying, which usually takes place by a face-to-face encounter, the defendant used the advantages of the Internet to attack his victims from a safe distance, 24 hours a day, while cloaked in anonymity."*

To change these offenders' immoral behaviours, they need to understand that bullying in all its manifestations is wrong and that those who indulge in it will face the consequences (Hinduja and Patchin 2019). Obtaining the assistance of law enforcement is the most popular strategy used to curtail these deviant online behaviours, and from a case study review, it was found that guardianships of this nature were 100% effective in protecting the victims. Despite some differences in country laws, the cyberbullying statute in most of the countries studied punishes *"the behaviours of posting or encouraging others to post on the Internet with the intent to intimidate or torment someone."* For instance, case #4 shows that *"The degree of participation of the accused in the offense was intense, prolonged, and only stopped due to the intervention of the victim's parents and law enforcement".*

Most people, on the other hand, frequently prefer punishment over discipline, therefore an appropriate sentence is necessary as a deterrent for cyberbullying behaviours.

However, laws alone cannot control people's immoral behaviour, it is crucial to educate people about how to use technology ethically and responsibly (Shariff, 2005). The key to reducing cyberbullying and unethical online behaviour is to uphold moral principles in both physical and virtual situations. These principles include respect for one another, being truthful, and refraining from taking others' information (Kaluarachchi et al. 2020). The counsel for the respondent related to case #10 also indicated that *"The Internet and, specifically, a social networking platform like Facebook readily enables the anonymous dissemination of information to a vast audience. The investigation of offenses is difficult and general deterrence is a major consideration."*

Therefore, most courts determine whether an offender is eligible to participate in certain treatment programs in addition to their sentences. These therapy programs are made to assist immoral offenders in reintegrating into society following their release. For instance, in case #12 *"The trial judge also ordered the defendant to complete 300 hours (about 2 weeks) of community service, attend counselling on cyberbullying and alternate lifestyles, and pay an assessment of $10,000, which would be allotted to a state-licensed or state-chartered community-based organization dedicated to providing assistance to victims of bias crimes"*. Case #7 is another notable example. The trial court ordered, *"that the offender's primary treatment target relates to improving emotional resilience and habituating himself to the uncertainty of relationships by increasing real-life social engagement."* These treatment programs include teaching them about cyber ethics and digital citizenship responsibilities as well as trying to uphold their moral values in both real-world and virtual contexts. Digital citizenship should be explicitly taught and trained in.

Furthermore, most courts often demand that offenders agree to a good behaviour bond for a period that varies based on the type of crime they committed. For instance*, case #6 "the respondent was sentenced to a total effective sentence of 3 years 6 months imprisonment to be released forthwith, upon entering into a recognizance in the sum of $500 to be of good behaviour for 3 years."* In case #15 *"The respondent was ordered to be released forthwith upon the respondent giving security by recognizance of $1,000 to comply with the condition imposed that the respondent be of good behaviour for a period of 24 months."* These good behaviour bonds are intended to protect offenders from breaking the law or acting in an antisocial manner in both physical and virtual settings upon their release.

In some cases, courts impose ICT/Internet restriction orders that prohibit offenders from posting messages using any communication media, including the Internet or a computer. Case #27 is a good example. The court has ordered the offender *"A six (6) month deferred custody and supervision order with, among others, the following conditions: (17) You shall delete your Facebook, Twitter, and Instagram accounts immediately (within 24 hours). (18) You shall not access any internet-based social media sites including but not limited to Facebook, Twitter, or Instagram during the entire term of this Order."* Case #8 is another example, the offender *"has been completely banned from accessing social networking sites such as Facebook."* Additionally, these limitations were put in place to discipline offenders for engaging in immoral online behaviour and stop further cyberbullying.

Effective laws and policies, cooperative learning strategies, community support programs, counselling, and consistent disciplinary measures are some of the effective ways to change the offender's immoral cyber behaviours and encourage the ethical and responsible use of technology in addressing cyberbullying.

5 Conclusion, Contribution, and Future Work

Cyberbullying is a complex form of bullying that is on the rise around the world. The growth and proliferation of social media platforms, as well as improved mobile technologies, smartphone accessibility, and Internet access, have significantly increased the potential for cyberbullying. People's health, educational rights, and psychological well-being can all be negatively impacted by cyberbullying in diverse ways. However, most of the current research on cyberbullying concentrates on the prevalence and predictors of cyberbullying, the comparison between cyberbullying and traditional bullying, or the risk and protective factors of cyberbullying. We have seen that preventive measures or strategies to prevent cyberbullying have received less attention. Therefore, the objective of this exploratory study was to investigate preventative or remedial measures for online deviant behaviour like cyberbullying.

The actions, methods, technologies, and best practices that can be employed to prevent or reduce this pervasive societal problem have all been suggested in this study. Regarding the victims, it's crucial that they comprehend how to use technology tools and platforms responsibly. It is essential to increase these

individuals' awareness of the risks and dangers associated with the Internet and social media platforms as well as to provide them with the knowledge, talents, and netiquette needed to navigate issues like cyberbullying. Some of the most effective technology-related remedies that can be used to safeguard the victims can be, blocking, and deleting identities/messages and/or accounts associated with cyberbullying. Additionally, it looked to be essential to use social media responsibly in order to stop or lessen cyberbullying.

From the standpoint of the offender, they must comprehend their obligations as digital citizens and cyber-ethics to change their immoral behaviours like cyberbullying. Since laws themselves cannot control people's immoral behaviour, it is important to educate people about how to use technology ethically and responsibly. Therefore, most courts determine whether an offender is eligible to participate in certain treatment programs in addition to their sentences. Effective laws, policies, cooperative learning strategies, community support programs, consistent disciplinary measures, and counselling programs are some of the effective ways to change the offender's immoral cyber behaviours.

The results of the study have implications in multiple ways: (1) they broaden the understanding of cyberbullying as a phenomenon, (2) identify the characteristics of victims, offenders and technology which facilitate cyberbullying (3) Finally, a better understanding of the preventive and reduction strategies of cyberbullying which can be used to develop of more targeted cyberbullying prevention and intervention programs. The research investigated in this paper has been limited by the dearth of studies on the responsible use of technology. Also, we could only locate a small number of court cases related to cyberbullying and the responsible use of technology. Future studies can focus on prevention strategies and measures that can be taken to safeguard people from online deviant behaviours like cyberbullying.

6 References

Agnew, R. 2014. "General Strain Theory," in *Encyclopedia of Criminology and Criminal Justice,* G. Bruinsma and D. Weisburd (eds.). New York, NY: Springer New York, pp. 1892-1900.

Alipan, A., Skues, J., Theiler, S., and Wise, L. 2020. "Defining Cyberbullying: A Multifaceted Definition Based on Perspectives of Emerging Adults," *International Journal of Bullying Prevention* (2).

Bandara, W., Furtmueller, E., Gorbacheva, E., Miskon, S., and Beekhuyzen, J. 2015. "Achieving Rigor in Literature Reviews: Insights from Qualitative Data Analysis and Tool-Support," *Communications of the Association for Information Systems* (37), pp. 154-204.

Burton-Jones, A., Bremhorst, M., Liu, F., and Trieu, V.-H. 2017. "It Use: Notes from a Journey from Use to Effective Use," in *The Routledge Companion to Management Information Systems*. Routledge, pp. 152-165.

Chan, T. K. H., Cheung, C. M. K., and Lee, Z. W. Y. 2021. "Cyberbullying on Social Networking Sites: A Literature Review and Future Research Directions," *Information & Management* (58:2), p. 103411.

Chan, T. K. H., Cheung, C. M. K., and Wong, R. Y. M. 2019. "Cyberbullying on Social Networking Sites: The Crime Opportunity and Affordance Perspectives," *Journal of Management Information Systems* (36:2), pp. 574-609.

Chen, L., Ho, S. S., and Lwin, M. O. 2017. "A Meta-Analysis of Factors Predicting Cyberbullying Perpetration and Victimization: From the Social Cognitive and Media Effects Approach." pp. 1194-1213.

Cocking, D., and Van den Hoven, J. 2018. *Evil Online*. John Wiley & Sons.

Coventry, L., Briggs, P., Blythe, J., and Tran, M. 2014. "Using Behavioural Insights to Improve the Public' S Use of Cyber Security Best Practices," G.O.f. Science (ed.). London,UK: Government Office for Science, pp. 1-20.

Elci, A., and Seckin, Z. 2016. "Cyberbullying Awareness for Mitigating Consequences in Higher Education," *Journal of Interpersonal Violence* (34).

eSafety Commissioner. 2020. "Pressures from Social Media." Retrieved 04/07, 2020, from https://www.esafety.gov.au/young-people/pressures-from-social-media

Facebook. 2020a. "Help Centre." from https://www.facebook.com/help

Facebook. 2020b. "Welcome to the Digital Literacy Library." *Digital Literacy Library* Retrieved 04/09, 2020, from https://www.facebook.com/safety/educators

Felson, M., and Clarke, R. 1998. "Opportunity Makes the Thief: Practical Theory for Crime Prevention," The Policing and Reducing Crime Unit (ed.). London.

Ghazawneh, A., and Henfridsson, O. 2013. "Balancing Platform Control and External Contribution in Third-Party Development: The Boundary Resources Model," *Information Systems Journal* (23:2), pp. 173-192.

Guo, S. 2016. "A Meta-Analysis of the Predictors of Cyberbullying Perpetration and Victimization.," *Psychology in the Schools* (53:4), pp. 432-453.

Hinduja, S., and Patchin, J. 2019. "Cyberbullying Identification, Prevention, and Response." Retrieved 10/06/2020, from https://cyberbullying.org/

Hinduja, S., and Patchin, J. W. 2009. *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying*. Thousand Oaks, CA: Sage Publications (Corwin Press).

Hinduja, S., and Patchin, J. W. 2010. "Bullying, Cyberbullying, and Suicide," *Archives of Suicide Research* (14:3), pp. 206-221.

Hoff, D., and Mitchell, S. 2009. "Cyberbullying: Causes, Effects, and Remedies," *Journal of Educational Administration* (47), pp. 652-665.

Huang, Q., Inkpen, D., Zhang, J., and Van Bruwaene, D. 2018a. "Cyberbullying Intervention Based on Convolutional Neural Networks," *Proceedings of the First Workshop on Trolling, Aggression and Cyberbullying (TRAC-2018)*, pp. 42-51.

Huang, Q., Singh, V., and Atrey, P. 2018b. "On Cyberbullying Incidents and Underlying Online Social Relationships," *Journal of Computational Social Science* (1).

Jenaro, C., Flores, N., and Frías, C. P. 2018. "Systematic Review of Empirical Studies on Cyberbullying in Adults: What We Know and What We Should Investigate," *Aggression and Violent Behavior* (38), pp. 113-122.

Kaluarachchi, C., Warren, M., and Jiang, F. 2020. "Responsible Use of Technology to Combat Cyberbullying among Young People," *Australasian Journal of Information Systems* (24).

Kowalski, R., Toth, A., and Morgan, M. 2017. "Bullying and Cyberbullying in Adulthood and the Workplace," *The Journal of Social Psychology* (158:1), pp. 64-81.

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., and Lattanner, M. R. 2014. "Bullying in the Digital Age: A Critical Review and Meta-Analysis of Cyberbullying Research among Youth," *Psychological Bulletin* (140:4), pp. 1073-1137.

Kowalski, R. M., Limber, S. P., and Agatston, P. W. 2008. *Cyberbullying: Bullying in the Digital Age*. Malden, MA: : Blackwell Publishing.

Kowalski, R. M., Limber, S. P., and McCord, A. 2019. "A Developmental Approach to Cyberbullying: Prevalence and Protective Factors," *Aggression and Violent Behavior* (45), pp. 20-32.

Lee, J., Abell, N., and Holmes, J. L. 2017. "Validation of Measures of Cyberbullying Perpetration and Victimization in Emerging Adulthood," *Research on Social Work Practice* (27:4), pp. 456-467.

Lianos, H., and McGrath, A. 2018. "Can the General Theory of Crime and General Strain Theory Explain Cyberbullying Perpetration?," *Crime & Delinquency* (64:5), pp. 674-700.

Livingstone, S., Haddon, L., Goerzig, A., and Ólafsson, K. 2011. "Risks and Safety on the Internet: The Perspective of European Children: Full Findings and Policy Implications from the Eu Kids Online Survey of 9–16 Year Olds and Their Parents in 25 Countries.." London, UK: EU Kids Online. London School of Economics & Political Science.

Lowry, P. B., Zhang, J., Wang, C., and Siponen, M. 2016. "Why Do Adults Engage in Cyberbullying on Social Media? An Integration of Online Disinhibition and Deindividuation with the Social Structure and Social Learning Model," *Information Systems Research* (27:4), pp. 962-986.

Lund, E. M., and Ross, S. W. 2017. "Bullying Perpetration, Victimization, and Demographic Differences in College Students: A Review of the Literature," *Trauma, Violence & Abuse* (18:3), pp. 348-360.

Moore, M. J., Nakano, T., Enomoto, A., and Suda, T. 2012. "Anonymity and Roles Associated with Aggressive Posts in an Online Forum," *Computers in Human Behavior* (28:3), pp. 861-867.

OECD. 2020. "Protecting Children Online: An Overview of Recent Developments in Legal Frameworks and Policies," Working Party on Security and Privacy in the Digital Economy (ed.). No. 295, OECD Publishing, Paris.

Perren, S., Corcoran, L., Cowie, H., Dehue, F., Garcia, D. J., Mc Guckin, C., Sevcikova, A., Tsatsou, P., and Völlink, T. 2012. "Tackling Cyberbullying: Review of Empirical Evidence Regarding Successful Responses by Students, Parents, and Schools," *International Journal of Conflict and Violence* (6), pp. 283-292.

Perren, S., Dooley, J., Shaw, T., and Cross, D. 2010. "Bullying in School and Cyberspace: Associations with Depressive Symptoms in Swiss and Australian Adolescents," *Child and Adolescent Psychiatry and Mental Health* (4:1), p. 28.

Pew Research Center. 2017. "Online Harassment 2017." Retrieved 01/04, 2021, from https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/

Polanco-Levicán, K., and Salvo-Garrido, S. 2022. "Understanding Social Media Literacy: A Systematic Review of the Concept and Its Competences," *Int J Environ Res Public Health* (19:14).

Raskauskas, J., and Huynh, A. 2015. "The Process of Coping with Cyberbullying: A Systematic Review," *Aggression and Violent Behavior* (23).

Rinta-Kahila, T., Someh, I., Gillespie, N., Indulska, M., and Gregor, S. 2021. "Algorithmic Decision-Making and System Destructiveness: A Case of Automatic Debt Recovery," *European Journal of Information Systems*), pp. 1-26.

Sabella, R., Patchin, J., and Hinduja, S. 2013. "Review: Cyberbullying Myths and Realities," *Computers in Human Behavior* (29), pp. 2703-2711.

Shariff, S., and Hoff, D. L. 2007. "Cyber Bullying: Clarifying Legal Boundaries for School Supervision in Cyberspace," *International Journal of Cyber Criminology* (1:1).

Slonje, R., Smith, P. K., and Frisén, A. 2013. "The Nature of Cyberbullying, and Strategies for Prevention," *Computers in Human Behavior* (29:1), pp. 26-32.

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., and Tippett, N. 2008. "Cyberbullying: Its Nature and Impact in Secondary School Pupils," *Journal of Child Psychology and Psychiatry* (49:4), pp. 376-385.

So, A., and Lenarcic, J. 2015. "Cross-Cultural Perspectives on Cyberbullying through Anethical Lens (Pending Publication)."

Sourander, A., Brunstein Klomek, A., Ikonen, M., Lindroos, J., Luntamo, T., Koskelainen, M., Ristkari, T., and Helenius, H. 2010. "Psychosocial Risk Factors Associated with Cyberbullying among Adolescents: A Population-Based Study," *Archives of general psychiatry* (67), pp. 720-728.

Spears, B., Keeley, M., Bates, S., and Katz, I. 2014. "Research on Youth Exposure to, and Management of, Cyberbullying Incidents in Australia: Part a – Literature Review on the Estimated Prevalence of Cyberbullying Involving Australian Minors (Sprc Report 9/2014)." Sydney: Social Policy Research Centre, UNSW Australia.

Twitter. 2019. "Everything You Need to Know So You Can Use Twitter Like a Pro." *Help Center* Retrieved 20/06, 2019, from https://help.twitter.com/en

United Nations Children's Fund. 2017. "The State of the World's Children 2017, Children in a Digital World." Califra: Germain Ake and Ernest.

Wang, Y. 2022. "Understanding the Role of Social Factors in Cyberbullying at Work," *Computers in Human Behavior* (134), p. 107325.

Williams, K. R., and Guerra, N. G. 2007. "Prevalence and Predictors of Internet Bullying," *Journal of Adolescent Health* (41:6), pp. S14-S21.

Zhang, S., Leidner, D., Cao, X., and Liu, N. 2021. "Workplace Cyberbullying: A Criminological and Routine Activity Perspective," *Journal of Information Technology* (37:1), pp. 51-79.