"Every Breath You Take I'll be Watching You": Governing Cyberstalking in Malaysia

Zaiton Hamin and Wan Rosalili Wan Rosli
Faculty of Law, Universiti Teknologi MARA, Malaysia

Keywords: Anti-Stalking Law, Cybercrime, Cyberstalking, Criminalisation, Motivation.

Abstract: Since the past decade, cyberstalking has been on the rise worldwide. The prevalence of such crime is much higher than its real-world counterpart due to the fact that computer users have unlimited connectivity to the Internet. Cyberstalking acts as a conduit to the commission of other illegalities such as identity theft, cyber fraud and physical danger such as rape and even murder. However, the nature of the crime and the perception on the adequacy of the law remains ambiguous in the current Malaysian legal landscape. Hence, this paper aims at examining the various motives of the cyberstalkers in committing such crime and the perception of the criminalisation of cyberstalking in Malaysia. This paper adopts a qualitative methodology, of which the primary data is generated from semi-structured interviews and secondary data from library-based sources. The preliminary findings revealed that several motivations of cyberstalkers were evident, including revenge and obsession. Significantly, there were paradoxical views on the adequacy of the current legal position for cyberstalking. The evidence from the findings illustrates the need for a review of the existing legal position, which does not adequately address the criminalisation of cyberstalking and the victims' protection within the Malaysian criminal justice system.

1 INTRODUCTION

In the last two decades, with the advent of information and communication technology (ICT), cybercrime has been on the rise worldwide. Cybercriminals are using such technology as a tool to commit cybercrimes that may transcend geographical boundaries. According to the recent Europol's Organized Crime Threat Assessment 2017, the Internet is the key facilitator for a majority of offline organised crime activities; for instance, criminals can quickly leverage the Internet to carry out traditional crimes such as distributing illicit drugs, sex trafficking and even stalking. Dolliver and Poorman (2018) suggests that cybercrime is a borderless problem where cybercriminals utilise anonymising technologies to commit Internet-facilitated crimes.

Within the global context, many jurisdictions have criminalised stalking not only in the real world but also in cyberspace, by amending their traditional laws. For instance, California became the first state in the USA to enact an anti-stalking law (Reyns, 2015). According to Vasiu and Vasiu (2013), the USA enacted its cyberstalking laws that explicitly include electronic forms of communications within the more traditional stalking laws. In 1997, the United Kingdom enacted its Protection from Harassment Act 1997 and New Zealand created the New Zealand Harassment Act in 1997 that covers both civil and criminal harassment (CCPL, 2013). Later in 2014, Singapore enacted its Protection from Harassment Act, which mirrors the UK 1997 Act (CCPL, 2013). In January 2017, Japan amended its anti-stalking legislation to include cyberstalking given that such crime is seen to be more dangerous than its real-world counterpart (Kyodo, 2017).

The Malaysian literature on stalking and cyberstalking is somewhat scarce. However, the early available literature appears to be focused on the unwillingness of female victims of cyberstalking to report such crime to the police (Haron, 2010). According to Cybersecurity Malaysia (2010), the actual number of cyberstalking victims is much higher because not all victims are willing to come forward with their reports. Cyberstalking has also been reported to be a severe threat, particularly to women and should not to be taken lightly (The Star, 2010). The recent local literature generally discussed the profile of stalkers and the victimisation of cyberstalking, rather than the legal aspects of

Hamin, Z. and Wan Rosli, W.
"Every Breath You Take I'll be Watching You": Governing Cyberstalking in Malaysia.
DOI: 10.5220/0010051803150320
In *Proceedings of the International Law Conference (iN-LAC 2018) - Law, Technology and the Imperative of Change in the 21st Century*, pages 315-320
ISBN: 978-989-758-482-4

governing the said crime (Indramalar, 2017). On such matters, Hamin and Wan Rosli (2017) contended that Section 233 of the Communications and Multimedia Act (CMA) 1998 may be used to prosecute cyberstalking and cyber harassment in Malaysia. The gap in the literature is that there has been no qualitative research undertaken to look into the perception of Malaysians on the current legal position, the motivations for cyberstalking and the sufficiency of the Malaysian laws to protect the victims. As such, this paper aims at examining the existing legal position in Malaysia and the various motives of cyberstalkers in committing such crime.

The first part of this article examines the literature of cyberstalking, the victimisation and motivation of the crime. While the second part reviews the legal position of the traditional and cyber laws in Malaysia on cyberstalking, the third part explains the methodology adopted by the researchers in conducting the research. The fourth part, which is the crux of the study, explains the preliminary findings. The discussion in the fifth section which discussed the relationship between the findings and the literature is next. The last section concludes the paper.

2 LITERATURE REVIEW

The literature suggested that stalking is an age-old offence in many parts of the world. Early literature defined stalking as a crime involving acts or behaviours of pursuit which is done over time, that is threatening and potentially dangerous towards the victim (Meloy, 1998). Similarly, Thomas (1993) argued that the main elements of stalking involved the repetitive and threatening conduct of the offender. Recent literature indicated that the crime appeared the same. For example, Nobles (2014) argued that stalking involved on-going harassment that is unwanted and causes fear or safety concerns towards the victim.

Cyberstalking is one of the types of cybercrime that have morphed from the traditional stalking to that in cyberspace, which may be committed through any electronic devices that are connected to the Internet (Leong, 2015). Recent literature indicated that cyberstalking is a prevalent crime and is becoming more dangerous than traditional stalking (Mutawa et al., 2016) due to the various crime stimuli of the Internet that provided tremendous opportunities to utilise advanced computer programs (Aa, 2011). With such technological development, the magnitudes of cyber harassment and cyberstalking are getting more prevalent and extensive (Leong, 2015).

On the issue of victimisation of such crime, more than 38 percent of cyberstalking victims fear that the offensive behaviour of cyberstalkers would develop into a face-to-face confrontation (Al-Khateeb and Epiphaniou, 2016). A recent US Bureau of Justice Statistics (2017) reported that within a year, an estimated 14 in every 1,000 persons aged 18 or older might become victims of cyberstalking. In 2013, a research conducted on the victimisation of stalking in Malaysia found that 26 percent of women had been stalked by their abusers (Indramalar, 2017).

The literature suggested that a wide range of motivation is currently influencing stalkers to stalk their victims in the real world and cyberspace. Bocij and McFarlane (2002) asserted that stalking is usually motivated by hate, revenge, power, and even racism. However, Lowry (2012) argued that the motivation of the offenders to commit cyberstalking ranged from jealousy of ex-partners to delusional fixation on the victims by stalkers. The literature, through mental profiling of cyberstalkers or online criminals, has identified not only the psychological factors that motivate them, but also the social factors involved (Jaishankar, 2011). The stalkers share traits such as envy, pathological obsession, including professional or sexual fixation, unemployment or failure with their job or life, and a cruel intention to intimidate or cause others to feel inferior (Mullen et al., 2000).

3 GOVERNING CYBERSTALKING IN MALAYSIA

In Malaysia, cyberstalking may be prosecuted under the traditional criminal law, which is the Penal Code, and the computer-specific law, which is the Communications and Multimedia Act 1998 (CMA 1998). Section 503 which is punishable with Section 506 of the Penal Code may accommodate stalking and cyberstalking as these sections cover criminal intimidation. Under Section 503, criminal intimidation is committed when a person threatens another with an injury to his person or body, with the intention of causing alarm to that person. The punishment under Section 506 is incarceration for a term that may extend to two years or a fine or both. To date, there are several cases of criminal intimidation; however, none of these cases involved stalking or cyberstalking. The existing cases prosecuted under Section 503 are generally concerned with inflicting physical violence on the victims. An example of these cases is *Zainuddin bin*

Mahmud v PP (2010) 7 MLJ 789, where the court found the accused guilty, as he criminally intimidated the complainant with injury when he threatened her with a parang and was sentenced to a fine of RM7000, which in default, would result in six months imprisonment. In *PP v Kenneth Francisco* (2000) MLJU 102, the defendant was charged with putting the victim in fear of injury by threatening to stab the latter. The court however acquitted and discharged the accused without his defence being called, as the prosecution had wrongly drafted the charge against him.

Apart from Section 503 on criminal intimidation, Section 351 on criminal assault and Section 354 on assault or using criminal force to a person with intent to outrage her modesty may also be applicable in prosecuting stalkers and cyberstalkers. If found guilty under Section 354, the offender shall be punished with imprisonment for a term, which may extend to ten years or fine or whipping or with any two such punishments. To date, there are about forty-seven cases reported under Section 354. An example of such cases is *Sha'Aribin A. Samat v PP* (2017) MLJU 5 which is concerned with the outrage of modesty of a schoolgirl by her teacher. The Sessions court found the defendant guilty and sentenced the defendant to three years of imprisonment. In another case of *PP v Mohd Rosli bin Ishak* (2017) 1 LNS 1390, the defendant was charged with Section 354 for outraging the modesty of his daughter by putting his hands in her underwear. The court sentenced the defendant for nine years and eleven months imprisonment and twenty-one strokes of rotan. However, there has been no prosecution for stalking or cyberstalking in both cases.

Section 233 of the CMA 1998 may be available to prosecute cyberstalking cases. Such section is concerned with acts and behaviours, whether continuous or repeated or otherwise, which are carried out through any network facilities, network services or applications to make, solicit or initiate the transmission of any comments, suggestions or other communication, which is obscene, indecent, false, menacing or offensive with the intent to annoy, abuse, threaten or harass another person (233(1)(a) CMA 1998). Section 233(1) (b) further provided that a person who initiates communication by using application services whether continuously or repeatedly, without disclosing his identity with the intention to annoy, abuse, threaten and harass any person at any number or electronic address may be found guilty under the said section. The penalty under Section 233 (3) of the CMA is a fine not exceeding fifty thousand ringgit or imprisonment for a term not exceeding one year or both. A person can also be further fined for one thousand ringgit for every day during which the offence continued after the conviction (Section 233(3) CMA 1998).

Despite the availability of Section 233 to prosecute the perpetrators of cyberstalking, up until today, no prosecution has been brought before the court for such cases. To date, there are only three cases that have been prosecuted under the said section. In the case of *Rutinin b. Suhaimin v PP* (2014) 5 MLJ 282 the defendant was found guilty after he had published a comment via his Internet account that states, "Sultan Perak Sudah Gila." However, the decision was overturned as there was evidence that anyone can access the defendant's account as his computer and his Internet account was accessible by other persons and on the day mentioned in the charge. In a recent case of *Nik Adib bin Nik Mat v PP* (2017) MLJU 1831, the accused was charged under Section 233(1)(a) of the CMA 1998 for posting pictures and comments regarding certain leaders on a website, which were offensive and false. The judge found the accused guilty and sentenced him to 1-week imprisonment term and a fine of RM3000. Another recent case is *Mohd Fahmi Redza bin Mohd Zarin v PP* (2017) MLJU 516 where the accused was charged for sending a false communication for the purpose of annoying others by using his Instagram account. However, the accused challenged Section 233 as unconstitutional, and the matter was postponed until the constitutional question was settled in the Federal Court.

Despite the utility of Section 233 in governing cyberstalking, it does not provide the necessary protections for the victims such as the protection order, restraining order, injunction, or any civil remedies, which are currently provided by the Protection from Harassment Act 1997 (PHA1997) in England and Wales. Also, this section does not identify or define the acts and behaviours that constitute cyberstalking or provide any instances of the impact of the stalkers' behaviour on the victim such as that provided under Sections 2A and 4A of the PHA 1997. In a Singaporean case of *PP v Colin Mak Yew Loong* (2013, Unreported), the defendant who had been sending threatening e-mails and voice messages for more than 6 years to the victim, including threats of violence by using an Ak-47 rifle and a lead pipe, was charged with criminal intimidation under Section 503 of the Singapore Penal Code and was sentenced to three years of imprisonment and SGD5000 fine under Section 506 of the Penal Code. This case had happened before the

creation of the Protection from Harassment Act 2014 (PHA 2014) in Singapore.

If a similar case were to be decided in Malaysia, a similar decision may apply since criminal intimidation in Singapore is in pari materia with Section 503 of the Malaysian Penal Code. However, if the case were decided in Singapore post-PHA 2014, the defendant would be charged with cyberstalking under Section 7 of the PHA 2014, where on conviction the accused can be liable for a fine not exceeding SGD$5,000 and imprisonment not exceeding the term or twelve months or both. If the harassment towards the victim continues after the conviction, the accused may also be charged for a subsequent offence with a maximum fine of SGD10, 000 or a maximum jail term of two years or both. A recent case in 2013 involving cyberstalking by a female perpetrator against her former boyfriend indicates a missed opportunity for the Malaysian court to decide on such crime as the victim brought the case in the course of action for cyber defamation (David Clayworth v Lee Chiang Yan, 2013 (Unreported)). Since 2010, after the break-up of her relationship with her boyfriend, Lee Chiang Yan, a Malaysian, relentlessly cyberstalked David Clayworth, a Canadian teacher. The accused posted numerous false posting on the Internet and some of which contained nude pictures of him with a caption 'Genital herpes'. The defendant also took over the victim's e-mail and Skype accounts and posted messages that the victim was a child molester, paedophile and preferred having sex with his students. The victim sued the defendant for defamation and won the case. The court ordered the defendant to pay RM66, 000 for damages. However, the online assault did not stop even after a contempt of court order was issued against her. Had the case been dealt with through the criminal law avenue and on a charge of cyberstalking, perhaps the court would have the opportunity to apply either the traditional criminal law or the CMA 1998 to decide this case.

4 METHODOLOGY

This research adopts a qualitative research, which would provide a deeper understanding of the social phenomena and a comprehensive overview of the subject matter under study (Silverman, 2013). Hence, such a methodology would enable the researcher to explore the views of the respondents on the criminalisation of cyberstalking in Malaysia and the motivations involved in such cybercrime. For the purpose of this paper, the preliminary findings are based on the data collection of both the primary and secondary data, and this stage is divided into two phases. The first phase is the library-based research or the literature review stage (Bell, 1987) in which all the relevant literature on cyberstalking, the legal position and the motivations for the said crime were examined. While the primary sources involve the CMA 1998 and the Penal Code, the secondary sources include textbooks, academic journal articles, government reports, newspaper articles and online databases and sources.

The second phase of the data collection is the fieldwork, in which the primary data is mainly generated from the face-to-face semi-structured interviews with the sixteen respondents. Bertaux (1981) and Guest, Bunce, and Johnson (2006) suggested that fifteen respondents would be the minimum sample size for qualitative research. The respondents of this research comprised of officers from the Royal Malaysian Police, CyberSecurity Malaysia, the Malaysian Bar Council representative, the Deputy Public Prosecutors from the Attorney General Chambers, legal practitioners and an NGO (Women Aid Organisation). Such interview method was chosen as it gives the researcher the opportunity to explore the respondents' opinions of the said issues in depth, rather than to test their knowledge or only to categorize it (Matt, 2000).

The sampling method in this research is purposive sampling, which means that the respondents were selected because they are likely to generate the useful data for the research (Crouch and McKenzie, 2006). The qualitative data analysis was conducted through thematic and content analysis, in which the observations and the interview transcripts from the semi-structured interviews were examined (Seidman, 2006). The process consisted of creating codes and categories, considering the themes and then analysing the respondents' perceptions and experiences, along with the literature review. The primary data were triangulated with the semi-structured interview data obtained from an officer from the Ministry of Communication and Multimedia and another officer from the Ministry of Women, Family and Community Development respectively. The said interviews were digitally recorded, and their contents were later transcribed and analysed using the Atlas.ti qualitative research software (Friese, 2014).

5 FINDINGS

The findings of this research on the motivations and the legal position in Malaysia on such crime are

explained below through the narratives of some of the respondents.

5.1 The Motivation of Cyberstalkers

The research revealed that obsession and attraction were believed to be the primary motivations of stalkers in committing cyberstalking. Obsessive stalkers are usually connected to a person who knows their stalkers such as an ex-lover, employer or from past relationships. Most of the respondents (10 out of 18) believed that cyberstalking was usually associated with obsession and attraction. A respondent stated that:

Cyberstalking happens when the stalker is a fan of the victim, he is obsessed with the victim and he thinks that he is in love with the victim.

The research also revealed that jealousy and humiliation were the principal motivations for stalkers, which confirmed the literature that such crime would usually happen, particularly when the stalkers know their victims or had past relationship with them. Jealousy and humiliation are from two different sides of the spectrum. The motivations normally develop when a stalker feels that he is being rejected by a victim. Some of the respondents (7 out of 18) believed that the stalkers' motivation to commit cyberstalking involved jealousy and humiliation. A respondent stated that:

Boyfriends and husbands who are overly jealous, always messaging their wives or girlfriends asking where they are and threatening them can turn into cyberstalkers.

Apart from that, the findings revealed that revenge may also be a motivating factor for stalkers. Similar to jealousy, such motivation may also be associated with the feelings of being rejected. The motivation for revenge is not limited to past relationships; it can also be for a current employer-employee relationship, neighbours, and even family members. A few of the respondents (4 out of 18) perceived that revenge may also be a factor for cyberstalking. A respondent stated that:

Sometimes, the motivation for cyberstalking is revenge. This usually happens when a stalker has information on a victim at their disposal. The stalker may use the information to stalk the victim out of revenge.

The findings also indicated that stalkers who suffer from pathological criminality have stalker traits build-in their genetic makeup, which motivated them to stalk their victims. The findings revealed that some of the respondents (8 out of 18) perceived that individuals who have pathological traits of a stalker mixed with criminogenic thinking were prone to commit cyberstalking. A respondent stated that:

When a perpetrator cyberstalks a victim, he must be mad. There must be something wrong with his mind; their brain is not functioning well because they are born that way.

5.2 The Adequacy of the Current Legal Framework

The findings revealed that there are paradoxical views on the adequacy of the current legal framework. On the one hand, most of the respondents (10 out of 18) perceived that the current legal framework was adequate to govern cyberstalking. A respondent from the enforcement an agency argued that:

If the crime does not fall under section 233 CMA, it can go under the Penal Code or the Sedition Act. If somebody is threatening the victim, she can report to the police.

Similarly, a respondent from a regulatory body highlighted that the current law was sufficient due to the availability of an existing legal framework involving four legislations that could govern cyberstalking. He commented that:

We have the Defamation Act, Sedition Act, Section 233 of the CMA and the Penal Code. The legal framework is there, and most of these Acts are more than enough. The current laws are adequate. We do not need more, as they can be abused. We need to utilize the existing laws that we have now.

On the other hand, some of them (8 out of 18) believed that the current law was inadequate. A respondent from an NGO stated that:

Some actions, such as threatening gestures and trespass, can be governed by the law. However, if they are messaging a victim constantly, following her around, causing her to fear for her safety, these actions are not covered by the law.

6 DISCUSSION

The evidence shows that cyberstalking is founded upon several motivations which may explain the motivation for the stalkers to stalk their victims. The findings suggested that obsession and attraction may drive the motivational factors that push a cyberstalker to stalk their victims. Interestingly, the findings also indicated that there is a perception that cyberstalkers may have pathological traits within their genetic makeup, which mean they are born with stalker traits. Such views are consistent with the literature, which indicated that obsession, jealousy, revenge, and

stalkers with pathological traits are the typical motivation for stalking (Jaishankar, 2011; Bocij and McFarlane, 2002; Mullen et al., 2000; Lowry, 2012)

The above findings also suggested that there are paradoxical views on the adequacy of the current legal framework in Malaysia. On the one hand, the findings show that there is a perception of the law being inadequate. Such a perception is in line with the recent local literature on cyberstalking, which suggested that such deficiency can be explained by the lack of specific provisions to address cyberstalking in the existing legislations. Also, it is due to the absence of provisions in the current legislations on any remedies or legal protection for the victims such as that in England and Wales. On the other hand, the findings indicated a perception that the legal framework in Malaysia is adequate and the futility of creating a new specific law to govern such crime. Unfortunately, such a view is inconsistent with the local literature that illustrated a significant rise of cyber harassment cases in the past years and the calls for a specific law to govern cyberstalking (Hamin and Wan Rosli, 2017; Indramalar, 2018, Cybersecurity Malaysia, 2010).

7 CONCLUSION

The findings indicated that various factors may explain the motives of cyberstalkers in committing the crime. In line with the extant literature, cyberstalking may usually be committed when there are elements of obsession, attraction, humiliation, jealousy, revenge and pathological traits within the stalkers. Also, contrary to local literature, the findings showed that there exist paradoxical views on the adequacy of the current legal framework. While some are optimistic of the existing laws in governing such crime, others are skeptical of such adequacy, which illustrates the necessity for a specific law to govern such crime.

The Malaysian legislations that may be utilised to deal with cyberstalking is in dire need of an immediate reform, which instrumentally may be in the form of an amendment to the Penal Code to include specific provisions for stalking and cyberstalking. Another idealistic form would be a stand-alone Act, which criminalises cyberstalking. In the long run, the absence of such legislation may pose severe mental and psychological impacts on the victims and, their family directly and indirectly on the nation. Malaysia should follow the footsteps of the UK to continuously enhancing and reviewing their anti-stalking legal framework to criminalise cyberstalking and holistically to provide effective legal protection for the victims.

ACKNOWLEDGEMENTS

This work was supported by the Law Faculty, Universiti Teknologi MARA, Shah Alam, Selangor, Malaysia.

REFERENCES

Al-Khateeb, H, Epiphaniou, G. (2016). How technology can mitigate and counteract cyberstalking and online grooming. *Computer & Security Journal*. pp: 14-18.

Bocij, P. and Mcfarlane, L. (2002). Online Harassment: Towards a Definition of Cyberstalking. *Prison Service Journal*, 139: 31-38.

Bertaux, D. (1981). *From the Life-History Approach to The Transformation of Sociological Practice.* Biography and Society: The Life History Approach in The Social Sciences 29–45. London: Sage.

Centre for Comparative and Public Law (2013). *Study on the Experience of Overseas Jurisdictions in Implementing Anti-Stalking Legislation*, Faculty of Law, The University of Hong Kong.

Crouch, M., McKenzie, H. (2006). The Logic of Small Samples in Interview-based Qualitative Research. *Social Science Information*. Vol. 45 No. 4 pp: 483-499.

Dolliver, D. S., &Poorman, K. (2018). Understanding Cybercrime. *Transnational Crime and Global Security* [2 volumes], 139.

Friese, S. (2014). *Qualitative Data Analysis with Atlas.ti*: Sage, p. 75.

Hamin, Z., Wan Rosli, W.R. (2017). ManagingCyberstalking in Electronic Workplaces*. International Conference on Business and Social Science (ICoBSS).* 20 February 2017 – 1 March 2017, Universiti Teknologi MARA Melaka, Melaka Malaysia.

Home Office. (18 January 2018). Stalking Protection Orders. Retrieved at https://homeofficemedia.blog.gov.uk/2018/01/18/home-office-in-the-media-18-january-2018/

Jaishankar, K. (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour*. Florida: Taylor & Francis Group.

Indramalar, S. (2017, 24 March). Crossing the Line. *The Star*. Retrieved at https://www.pressreader.com/malaysia/the-star-malaysia-star2/20170324/281479276240629.