Available Online at www.e-iph.co.uk
Indexed in Clarivate Analytics WoS, and ScienceOPEN

E-B Environment - Behaviour Proceedings Journal

CSSR 2017

https://www.amerabra.org; https://fspu.uitm.edu.my/cebs; https://www.emasemasresources.com
4th International Conference on Science & Social Research
The Pines, Malacca, Malaysia, 06 -07 December 2017

e-IPH e-International Publishing House Ltd., United Kingdom

Whither the Protection for Cyberstalking Victims? Some evidence from Malaysia

Zaiton Hamin, Wan Rosalili Wan Rosli

Faculty of Law, Universiti Teknologi MARA, Shah Alam, Selangor, Malaysia

zaiton303@uitm.edu.my, rosalili@uitm.edu.my

Abstract
Cyberstalking leads to a chain of reactions such as identity theft, rape, and even murder. Despite the severe ramifications of cyberstalking, the perception of the adequacy of the law and the legal protection for victims remain ambiguous. This paper aims at examining the perception of the criminalisation of such crime, the gendered nature of such crime and the attendant legal protection for its victims. This paper adopts a qualitative methodology. The preliminary findings revealed that such crime is not considered as a gendered crime and there exists ambivalence on the perception of the crime and the legal protection of victims.

Keywords: Cyber Stalking, Criminalisation, Gender, Secondary Victimisation, Victim-Blaming Mentality

DOI: https://doi.org/10.21834/ebpj.v5iSI1.2297

1.0 Introduction

Stalking is a crime that has become ubiquitous for the past two decades. With the convenience and accessibility provided by information and communication technology (ICT), the dark side of such crime is re-emerging. Such crime that was once committed in the real-world has now transcended into cyberspace. Stalking which was once thought to be a real-world crime is now considered to be more dangerous if committed online. Within the global context, many jurisdictions have criminalised cyberstalking. The first state in the USA to criminalise cyberstalking is California in 1992 (Vasiu and Vasiu, 2013). Other jurisdictions such as the UK and New Zealand enacted their anti-stalking laws in 1997 in the form of the Protection from Harassment Act 1997 and the New Zealand Harassment Act 1997 respectively. These statutes cover both criminal and civil harassment (CCPL, 2013). Singapore followed the UK's footsteps by criminalising cyberstalking and created the Protection from Harassment Act in 2014 (Hamin & Wan Rosli, 2016). The anti-stalking laws in the UK, Singapore, and the United States offer various protections for the stalking victims such as protection order, injunction, damages and restraining orders (Middlemiss, 2009; Cheong, 2014).

The extant literature on cyberstalking indicates that the veil of anonymity attracts stalkers to stalk their victims in cyberspace (Reyns, 2011, Ahlgrim, 2015, Heinrich, 2015, Middlemiss, 2014). Leong (2015), Heinrich (2015), Reyns (2011) and Tavani and Grodzinsky (2002), suggest that cyberstalkers can operate anonymously or pseudonymously while online, and they can stalk one or more individuals from the comfort of their home without having to venture out into the physical world to commit such crimes. Studies have shown that women are most likely to be stalked rather than men in traditional stalking and cyberstalking, which implies that such crime is mainly a gender-motivated crime towards women committed by men (Godwin, 2003, Medlin, 2002, Reyns, 2010, Nobles, 2013).

The literature in Malaysia on the criminalisation of cyberstalking is somewhat scarce. The recently available research indicates that the traditional criminal law in the Penal Code and cyber law in the shape of the Communication and Multimedia Act 1998 are the legal responses to cyberstalking in Malaysia (Hamin and Wan Rosli, 2017). Other local literature highlights the unwillingness of female cyberstalking victims to report the crime to the police (Haron, 2010). Similarly, CyberSecurity Malaysia states that the problem posed by cyberstalking is peripheral as the actual number of the victim is higher because not all victims are willing to come forward with their

eISSN: 2398-4287 © 2020. The Authors. Published for AMER ABRA cE-Bs by e-International Publishing House, Ltd., UK. This is an open access article under the CC BYNC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/). Peer–review under responsibility of AMER (Association of Malaysian Environment-Behaviour Researchers), ABRA (Association of Behavioural Researchers on Asians) and cE-Bs (Centre for Environment-Behaviour Studies), Faculty of Architecture, Planning & Surveying, Universiti Teknologi MARA, Malaysia.
DOI: https://doi.org/10.21834/ebpj.v5iSI1.2297

reports (CyberSecurity Malaysia, 2010). However, the problem with the literature is that there has been little research to examine the criminalisation and the legal protection available for cyberstalking victims in the country. As such, this paper seeks to examine such protection for cyberstalking victims under the current laws in Malaysia and intends to fill in the gap in the literature.

The first part of this paper examines the literature on cyberstalking, the gendered nature of the crime and its effects. While the second part reviews the legal position of the anti-stalking laws in Malaysia, 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 discusses the relationship between the findings and the literature is next. The last section concludes the paper.

2.0 Literature Review

Cyberstalking is defined as a collection of behaviours whereby a person uses ICT such as e-mail, forums, blogs and social networking websites to repeatedly harass and pursue another person, which causes alarm or fear towards the latter (Mutawa, 2016). Cyberstalking behaviours include intimidating, accusing, monitoring and also impersonating the victims (Mutawa, 2016). The Australian Institute of Criminology (2016) defines cyberstalking as persistent behaviours that instil apprehension and fear within a virtual environment. Smoker and March (2017) contend that cyberstalking becomes more normalise than before due to technological development, which provides greater avenues of communication and open access to information as well as the susceptibility for disinhibited behaviour within cyberspace.

Commentators suggest that cyberstalking may be more dangerous and prevalent than traditional stalking due to the various crime stimuli of the Internet that provide tremendous opportunities to utilise advanced computer programs (Aa, 2011; Mutawa, 2016). Cyberstalkers have no difficulty in finding their victims which can be done with a click of a button. The chances of being confronted with their actions are negligible as they would conceal their identities, alter critical data, move and delete the information within seconds and destroy the evidence (Aa, 2011). Rawlinson (2015) contends that in Australia, 98 per cent of domestic violence victims have also experienced cyberstalking. Al-Khateeb and Epiphaniou (2016) argue that more than 38 per cent of cyberstalking victims fears that the offensive behaviour of the offenders online would develop into a face-to-face confrontation. Tokunaga and Aune (2015) suggest that the threat of cyberstalking has become imminent and state that about 20 per cent to 40 per cent of Internet users are victimized through cyberstalking. The US Bureau of Justice Statistics (2017) reports that within a year, an estimated 14 in every 1,000 persons aged 18 or older may become victims of cyberstalking. The recent statistics compiled by the Malaysian Computer Emergency Response Team (MyCERT) on cyber harassment incidences in Malaysia shows the numbers have tripled in the last ten years (MyCERT, 2016). The latest number of such crime reported by MyCERT for the first half of the year 2017 is 406 cases. It indicates an increase in the number of cases as 529 cases were reported in 2016 and 442 cases in 2015.

The literature on the extent of female victimisation in cyberstalking suggests that the majority of stalking victims are women and the majority of perpetrators are men (Godwin, 2003; King-Ries, 2001; Reyns, 2012; Aa, 2011). The UK National Stalking Helpline (2011) statistics shows that the majority (80 per cent) of cyberstalking victims are female and the majority 70.5 per cent) of perpetrators are male. (The British Office for National Statistics (2015) reported that from 2014 to 2015, twice as many women rather than men reported having experienced stalking, which is more than 1.4 million female victims. Also, the US Bureau of Justice Statistics (2017) reported that women in the USA are greater at the risk of stalking victimisation. However, the accuracy of such statistics was doubted as no proper data on the victims of stalking and cyberstalking are made available (Mutawa, 2016). Heinrich (2015) explains the rationale for such victimisation and argues that women have a higher percentage of victimisation in cyberstalking rather than men as women tend to spend more time online.

Regulating Cyber Stalking in Malaysia

In Malaysia, the law that may regulate cyberstalking comprises of the Communication and Multimedia Act 1998 (CMA 1998) and the Penal Code. Section 233 of the CMA 1998 governs the improper use of network facilities or network services. A person who commits an offence under this section shall on conviction be liable to 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. However, no such cases relating to cyberstalking have ever been prosecuted under this section. The only case that is reported on this section is the case of Rutinin b Suhaimin v PP (2014) 5 MLJ 282 whereby the accused had published a comment that 'Sultan Perak sudah gila !!!!!' via his Internet account. The decision, in this case, was overturned by the higher court as there was evidence that other persons could access the accused's account as his IP line was on continuous login the whole day on the day the crime was committed. 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 and civil remedies which are provided under 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 those provided under Sections 2A and 4A of the PHA 1997.

Section 503 and 506 of the Penal code which provides for criminal intimidation may also govern cyberstalking. Criminal intimidation is committed when a person threatens another with an injury to his person with the intent to cause alarm to that person. The punishment for criminal intimidation under Section 506 is imprisonment for a term that may extend to two years or fine or both. To date, 11 cases of criminal intimidation have been prosecuted in the courts, but none of those cases involves stalking or cyberstalking. In the Singaporean case of PP v Colin Mak Yew Loong (2013, Unreported), the defendant who has been sending the victim threatening e-mails and voice

messages for more than 6 years, including threats of violence by using an Ak-47 rifle and a lead pipe, was charged for criminal intimidation and was sentenced to three years of imprisonment and SGD5000 fine. This case happened before the implementation of the Protection from Harassment Act 2014 (PHA 2014) in Singapore. If the case were decided in Malaysia, the same decision would apply as criminal intimidation in Singapore is in pari materia with Section 503 of the Malaysian Penal Code. However, if the case were decided post-PHA 2014, the defendant would have been charged with cyberstalking under section 7 of the PHA 2014 whereby on conviction the accused can be liable for a fine not exceeding SGD5,000 and imprisonment not exceeding the term of twelve months or both. If the harassment towards the victim continues, 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.

Parliament had recently amended the Domestic Violence (Amendment) Act 2017, which introduced an Emergency Protection Order (EPO) that allows social welfare officers to grant the victims immediate protection against their abusers (Ministry of Women, Family and Community Development, 2017). The victims need not make a report to the police or a court order to obtain the EPO which is valid for seven days (Section 3A Domestic Violence (Amendment) Act 2017). There is also the Interim Protection Order (IPO) under section 4 of the new Domestic Violence (Amendment) Act 2017, whereby victims are required to lodge a police report for the IPO to be granted. However, such legal protection against the abusive stalkers is only available to victims who are in marital and familial relationships. Therefore, such protection is not holistic and does not provide full protection for the numerous cyberstalking victims who are outside such a relationship.

3.0 Methodology

This research adopts qualitative research, which would provide a deeper understanding of the social phenomena and a holistic 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 and the legal protection of victims of cyberstalking in Malaysia. 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 step is the library-based search or the literature review stage (Bell, 1987) in which all the relevant literature on cyberstalking and the gendered nature of the crime were examined. While the primary sources involve the Communication and Multimedia Act 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) suggest that fifteen respondents would be the minimum sample size for qualitative research. These respondents comprised of the 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 allows the researcher to explore the participant's opinion of an issue 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 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 by an officer from the Ministry of Communication and Multimedia and the Ministry of Women, Family and Community Development respectively. The said interviews were digitally recorded, and their contents have been transcribed and analysed using the Atlas. ti qualitative research software.

4.0 Preliminary Findings

The research is currently at the preliminary stage of data analysis, in which the full findings have yet to be extracted from the primary data. However, for this paper, some preliminary findings on the criminalisation and the legal protection of victims of cyberstalking could be obtained as below.

Secondary Victimisation in Cyber Stalking Perception

The research revealed that on the perception of cyberstalking, there appeared to be ambivalence on the seriousness of cyberstalking. Despite understanding the nature of cyberstalking, the majority of the respondents were either unaware of the seriousness of the offence or were engaging in what could be considered as secondary victimisation of cyberstalking. One respondent stated that:

I believe that when someone sends you SMS or WhatsApp or e-mail message many times in a day threatening you, that is cyberstalking…it is a serious crime… however, I'm not too sure how many Malaysian are experiencing such a thing.

Minimising the severity of the threats

Some of the respondents, in particular, the regulators, seemed to consider such offence lightly and suggested that a simple solution could be obtained and that such an offence could be easily tackled. A respondent stated that:

It's easy, the victim need only to close her account. They could also create a new account and make sure that the stalker is no more in the friend's list.

Another respondent suggested that:

If you just grow up and ignore the stalkers, you will be OK.

Victim-blaming mentality

Some of the respondents even blame the victims for exposing themselves to cyberstalkers. A respondent from the regulatory body remarked that:

If you are the one who opens up everything to the public… then it's your problem.

On a similar assertion of victim-blaming, another respondent argued that:

You would not open yourself up to the public in real life without cause, and similarly, there is no reason for you to open yourself to the anonymous Internet.

Non-gendered Crime

The findings revealed that the majority of the respondents thought that the perpetrators of the crime were not mainly men as they believed that both men and women were potential cyberstalkers. A respondent from the regulatory body remarked that:

The stalkers can be anyone, not necessarily men.

Such belief appeared to be based on the equal percentage of Internet users between the genders. Another respondent from the same regulatory body suggested that:

In Malaysia, our Internet users are almost 50-50...54/46 that means, we have an equal number of users for female and male…I don't think the crime is limited to gender because technology is gender-neutral.

The Legal Protection for Victims

The findings suggested not only there were paradoxical views on the sufficiency of the available laws to cover cyberstalking, but also on the adequacy of the legal protection provided by the current laws for the victims of cyberstalking. A respondent from a legal firm remarked that:

Cyberstalking is a crime under the existing law… similar reliefs are available under the Domestic Violence Act, and under the Rules of Court 2012 and by common law (e.g., quia timet injunctions).

Another respondent contended that:

Seriously I cannot see what protection is provided to the victims with the kind of law that we have now.

Another respondent from the regulatory body wrongly suggested that:

Currently, I think you still can avail yourself to this kind of protection through the Penal Code…because the Penal Code provides what we call restraining orders and all that.

Also, the findings showed that there was ambivalence on the possibility of creating a legal modality to protect cyberstalking victims. While some of the respondents were somewhat favourable to the creation of a specific law to provide for the legal protection of cyberstalking victims such as those available in England and Wales, others were sceptical of this legal endeavour. A respondent from the regulatory body remarked that:

We need to come out with that kind of protection available in the UK. I think that when we create a law on stalking it must come together with the necessary protection. It's good.

Another respondent cautioned that:

In the Malaysian environment, I don't think we can create a new law on cyberstalking. The ministry has its priority on the law they want to establish.

5.0 Discussion

The preliminary findings indicated that there was ambivalence on the perception of cyberstalking. On the one hand, the said crime was perceived to be serious, but on the other hand, the apathy shown to the victims was surprising. The evidence suggested that the majority of the respondents were not fully aware of the effects of cyberstalking. Interestingly, the nonchalant responses to such crime such as closing the victim's account or ignoring the stalker further indicated the lack of knowledge on the seriousness of the crime and its inherent dangers.

The above findings indicated that the majority of the respondents believed that cyberstalking is not a gender-motivated crime, and anyone can be a cyberstalker. Such a view is contrary to the above-mentioned current literature which showed that men are the more likely perpetrator than women (The Bureau of Justice Statistics (2017); the British Office for National Statistics, 2015; Godwin, 2003; King-Ries, 2001; Reyns, 2012; Aa, 2012). Similarly, the findings seem to disprove the Strategy and Policy Directorate research (2014) that women are more vulnerable to the victimization of cyberstalking rather than man.

With regards to the lack of legal protection for cyberstalking victims, the findings again indicated that the paradoxical perception existed amongst the respondents. While some of the respondents believed that a specific law on cyberstalking was an illusion, there was also favouritism on a specific law modelled on that in England and Wales with some legal protections provided within. Such ambivalence on the adequacy of the law and its legal protection seemed to be contrary to the international and local literature mentioned above on the sufficiency of the law dealing with such crime (Hamin and Wan Rosli, 2017; Mutawa et al., 2016).

6.0 Conclusion

The preliminary findings indicated that there was ambivalence on the perception of the said crime in which there was secondary victimisation of the victims in the form of victim-blaming and minimizing the threats of cyberstalking. Also, contrary to the extant literature, the findings showed that such a crime was not considered a gendered crime. Importantly, the findings suggested the paradox of the sufficiency of the law and its attendant legal protection for the victims. Also, the mixed views on the legal mechanism or modality to cater for the legal protection for the victims were in evident.

The Malaysian legal framework on cyberstalking is in dire need of an immediate review so that new provisions or a new law could be created to provide adequate protection and remedies to the victims of cyberstalking regardless of their gender and relationship status. Another idealistic form would be a stand-alone Act, which criminalises cyberstalking. In the long run, the absence of specific 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 enhance and review the anti-stalking legal framework to criminalise cyberstalking and holistically to provide adequate legal protection for the victims. Unless and until a political will exist to protect the victims of such crime, the future of such victims appears bleak. Until such time, the question remains, whither the legal protection for cyberstalking victims?

Acknowledgments

This work was supported by research grant FRGS/1/2016/SSI10/UITM/02/5 by the Research Management Centre, UiTM Shah Alam, Selangor.

References

Australian Institute of Criminology (2016). Cyber stalking.
Retrieved at http://www.aic.gov.au/crime_types/cybercrime/onlinevictimisation.html.

Al-Khateeb, H, Epiphaniou, G. (2016). How Technology Can Mitigate and Counteract Cyber Stalking and Online Grooming, Computer & Security Journal, pp: 14-18.

Ahlgrim, B. M. (2015). Cyber Stalking: Impact of Gender, Cyber Stalker – Victim and Proximity. (Unpublished doctoral thesis). University of North Dakota.USA.

Aa, S. (2011). International (Cyber) Stalking. R. M. Letschert, & J. J. M. van Dijk (Eds.), The new faces of victimhood: Globalization, transnational crimes and victim rights. (pp. 191-213).

Bureau of Justice Statistics (2017). Stalking and Cyber Stalking. Office of Justice programs. Retrieved at https://www.bjs.gov/index.cfm?ty=tp&tid=973.

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.

Guest, G., Bunce, A., Johnson, L. (2006). How Many Interviews Are Enough? An Experiment with Data Saturation and Variability. Field Methods. Vol. 18 No. 1 pp: 59-82

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

Hamin, Z., Wan Rosli, W.R. (2016). Managing the Risk of Cyber Harassment @ Work. The 8th International Management and Accounting Conference (IMAC8), 28-29 September 2016, Adya Hotel. Langkawi Island, Malaysia.

Heinrich, P., A. (2015). Generation iStalk : an Examination of the prior relationship between victim of stalking and offenders, Theses, Dissertations and Capstones, Paper 917

Haron, H., Yusof, F. (2010). Cyber stalking: the social impact of social networking technology. International Conference on Education and Management Technology (ICEMT 2010).

Bell, J. (1987). Doing Your Research Project – A Guide for First-Time Researchers in Education and Social Science. Philadelphia: Open University Press.

Mutawa, N., Bryce, J., Fanqueira, V., Marrington, A. (2016). Forensic Investigation of Cyberstalking Cases Using Behavioural Evidence Analysis. Digital Investigation, vol. 16 pp: 96-103.

Medlin, A., N. (2002). Stalking to Cyber stalking, a Problem Caused by the Internet, Law and the Internet, Fall 2002 papers, Georgia State University College of Law, 140.

Matt, S. (2000). Qualitative Interviewing, In Dawn Burton (ed.). Research Training for Social Scientists. London: SAGE Publications.

Smoker, M., March, E. (2017). Predicting perpetration of intimate partner cyberstalking: Gender and the Dark Tetrad. Computers in Human Behavior, 72, 390-396.

Silverman, D. (2013). Doing Qualitative Research. Los Angeles: SAGE.

Seidman, I. (2006). Interviewing as Qualitative Research. New York: Teachers College Press.

Tokunaga, S., Aune, K. (2015). Cyber Defense: A Taxonomy of tactics for Managing Cyberstalking. Journal of Interpersonal Violence. Pp: 1-25.

Vasiu, I., Vasiu, L. (2013). Cyberstalking Nature and Response Recommendations, Academic Journal of Interdisciplinary Studies. Vol. 2 No. 5 pp: 226-234.