INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 11, Issue 6, (2021) E-ISSN: 2222-6990

Non-Criminalisation of Cyberstalking and Its Impact on Justice for Victims: Some Evidence from Malaysia

Wan Rosalili Wan Rosli[1], Zaiton Hamin[2], Ahmad Ridhwan Abd Rani[3], Saslina Kamaruddin[4] & Rafizah Abu Hassan[5]

[1, 3, 5]Senior Lecturer, Faculty of Law, UiTM Shah Alam, Selangor, Malaysia, [2]Associates Professor, Faculty of Law, UiTM Shah Alam, Selangor, Malaysia, [4] Senior Lecturer, Faculty of Economics and Management, UPSI, Perak, Malaysia

Email: rosalili@uitm.edu.my

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v11-i6/10336 DOI:10.6007/IJARBSS/v11-i6/10336

Published Date: 09 June 2021

Abstract

In the digital era, some real-world crimes have now transcended into cyberspace. Cybercrime such as cyberstalking is one of them and is considered as an emerging threat in Malaysia. Its prevalence in the reported statistics is merely a tip of an iceberg as many cases may not be reported. Cyberstalking may lead to a chain of psychological trauma and more severe crimes such as identity theft, rape, and even murder. However, despite its serious ramifications, the absence of any specific law to curb such criminality is regrettable and glaring in the Malaysian legal landscape. Hence, this paper aims at examining the technological and social factors contributing to such illegality, the rationales for the non-criminalisation and its implication for the victim's sense of justice. This paper adopts a qualitative methodology, of which the primary data is generated from semi-structured interviews with relevant respondents. The data triangulation is obtained from experts at two relevant ministries. The secondary data are the relevant cyber law, the Penal Code, books, academic journals, online databases and library-based sources. The findings revealed that the catalysts for cyberstalking are varied and that such crime has not been specifically criminalised in the Malaysian cyber laws or traditional legal framework. Such a legal lacuna calls into question not only the adequacy of the current law in dealing with such crime but also the availability of legal protection and non-denial of justice for cyberstalking victims as envisaged by the National Cyber Security Policy 2006 and the Sustainable Development Goals No.16.

Keywords: Cyberstalking, Causal Factors, Manufactured Risks, Criminalisation, Individual Responsibility, Victims, Justice

Introduction

Since the past two decades, real-world harassment and stalking have become ubiquitous. The advent of information and communication technology (ICT), particularly the Internet and its

applications, such as the social media platform, has led the dark side of such crime to re-emerge. Once committed in the real world, it has now transcended into cyberspace and is now considered to be more dangerous when committed online. On the prevalence of such crime, MyCERT incident reports show that cyber harassment incidences, including cyberstalking, have considerably increased in the last six years, which in turn suggests the emerging threats the said crime is posing to Malaysians. The figures in 2015 were 442, in 2016 it increased to 529 and 560 in 2017. In 2018 the number of cases reported was 356, and 260 in 2019 and up until July 2020, it has reached 337 cases. The downward trend of cases reported in 2018 and 2019 was due to under-reporting by victims as highlighted by (CyberSecurity Malaysia, 2020).

Within the global context, the extant literature on cyberstalking suggests that the veil of anonymity attracts stalkers to stalk their victims in cyberspace (Fissel & Reyns, 2020; Kalaitzaki, 2020; Ahlgrim, 2015; Heinrich, 2015; Middlemiss, 2014). Papakitsou (2020); Leong (2015); Reyns (2019) and Tavani and Grodzinsky (2002), suggest that the Internet anonymity makes it easy for cyberstalkers to operate anonymously or pseudonymously, enabling them to stalk numerous victims from the comfort of their home without having to venture out into the physical world. Studies on traditional stalking and cyberstalking have shown that women are most likely to be stalked rather than men, which implies that such crime is mainly a gender-motivated crime towards women committed by men (Godwin, 2003; Medlin, 2002; Reyns, 2019; Nobles, 2013).

Currently, many jurisdictions around the world have criminalised real-world stalking as well as cyberstalking. California became the first state in the USA to criminalise stalking in 1992 (Vasiu and Vasiu, 2013). Other jurisdictions such as England and Wales and New Zealand enacted their anti-stalking laws in 1997 in the form of the Protection from Harassment Act (PHA) 1997 and the New Zealand Harassment Act 1997 respectively. These statutes cover both criminal and civil harassment (CCPL, 2013). Singapore followed the English and Welsh footsteps by criminalising cyberstalking and created the Protection from Harassment Act in 2014 (Hamin & Wan Rosli, 2016 & 2020). The literature indicates that the anti-stalking laws in England and Wales, Singapore, and the United States offer various protections for the stalking victims such as protection order, injunction, damages and restraining orders (Todd, Bryce & Franqueira, 2020, Middlemiss, 2009; Cheong, 2014).

Within the local legal terrain, the literature on the criminalisation of cyberstalking let alone the protection for cyberstalking victims is relatively 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 possible legal responses to cyberstalking in Malaysia (Hamin & Wan Rosli, 2017 & 2020). Other local literature highlights the unwillingness of female cyberstalking victims to report the crime to the police (Haron, 2010). Similarly, the report from CyberSecurity Malaysia suggests cyberstalking is merely the tip of the iceberg and hence, peripheral as the actual number of the victims is higher because not all victims are willing to come forward to report their victimisation (CyberSecurity Malaysia, 2019). It is within this context and issues that this paper seeks to examine the factors affecting the risks of being cyberstalked, the raison d'être for the failure of the Malaysian Government to criminalise such crime and its impact on justice for its victims. As such, this paper intends to fill in the gap in the literature on cyberstalking in Malaysia.

The first part of this paper examines the legal position of cyberstalking in the existing Malaysian statute book. The second part explains the methodology adopted by the researchers in conducting the research. The third part, which is the crux of the study, explains

the findings on the drivers for such criminality, the rationales for the lack of its criminalisation and its impact on the victim's legal protection. The discussion in the fourth section discusses the relationship between the findings and the literature before the last section concludes the paper.

The Legal Position on Cyber Stalking in Malaysia

The laws that expressly regulate stalking and cyberstalking are deficient. However, there is a legal framework comprising the traditional criminal law and cyber law that may be applicable to deal with cyberstalking, involving the Communication and Multimedia Act 1998 (CMA 1998) and the Penal Code. Section 233 of the CMA 1998 governs improper use of network facilities or network services. The penalty for such crime is a maximum fine of fifty thousand ringgit or a maximum of one-year imprisonment 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)). However, no cyberstalking cases have ever been prosecuted under this section. Despite the utility of section 233 in governing cyberstalking, it lacks 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 (PHA)1997 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 section 2A and 4A of the PHA 1997.

On the traditional criminal law front, section 503 and section 506 of the Penal Code, which provide for criminal intimidation may cover cyberstalking. Criminal intimidation is committed when a person threatens another with any personal injury with the intent to cause alarm to that person. The punishment under section 506 is a maximum of two years imprisonment or fine or both. To date, 11 cases of criminal intimidation have been prosecuted, but none of those cases involve stalking or cyberstalking. However, these sections appear to be too broad as it covers various types of threats to a person. Similar to the CMA 1997, it does not explicitly refer to stalking or cyberstalking. Section 507 of the Penal Code which covers criminal intimidation by anonymous communication may also apply to govern cyberstalking. Section 507 is said to be an aggravated offence of section 506 and provides a more severe punishment as the offence causes a greater alarm to the victim than section 506. The penalty is a maximum imprisonment of two years, in addition to section 506 penalty. However, similar to section 503, this section does not expressly refer to stalking in the real world or cyberspace.

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 researchers to explore the views of the respondents on the causal factors of cyberstalking, the criminalisation and the legal protection of victims of cyberstalking in Malaysia. The findings are based on the data collection of both the primary and secondary data, and this stage is divided into two phases. The first stage is the literature review stage (Bell, 1987) in which all the relevant literature on cyberstalking and its legislation, including the victim's protection, are analysed. The primary sources are the Communication and Multimedia Act 1998 and the Penal Code, and 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. The respondents were 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). The primary data was triangulated with 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 researchers chose the interview method as it allowed the researchers to explore the participant's opinion of the issue in-depth, rather than to test their knowledge or only to categorise it (Matt, 2000). The sampling method in this research is purposive sampling, in which the respondents were selected because they are likely to generate useful data for the research (Crouch and McKenzie, 2006).

The researchers digitally recorded the said interviews, transcribed and analysed their contents using the Atlas.ti qualitative research software. The researchers then conducted the qualitative data analysis through thematic and content analyses, in which we examined the observations and the interview transcripts from the semi-structured interviews (Seidman, 2006). This process consisted of creating codes and categories, considering the themes and then analysing the respondents' perceptions and experiences, along with the literature review. After the data analysis and after further analysis with the legal literature, the existing legislation and cyberstalking literature, we obtained the findings, which will be discussed below.

Findings

Factors Contributing to Cyberstalking Risks

Technological Advancement

The findings revealed that several factors might generate the risks of cyberstalking involving the inter-action of technology or machine, human factors and the process of controlling or managing the security perimeters. Most respondents believed that technological advancement had created new risks to users, including cyberstalking risks, particularly with the availability of the Internet and social media platforms. A respondent noted that:

> ICT development and Internet access are the reasons why crimes such as cyberstalking have become more prevalent.

Availability of Stalking Tools on the Internet

The findings showed that the availability of new technology and software such as spyware, which could be downloaded for free or for a low price on the Internet enable stalkers to track their victims and gather information on them. A respondent stated that:

> Technology has evolved. Spy tools can be retrieved quickly and can be bought over the Internet, which can be used to stalk any victim. The spyware tools can also be used to follow where a victim goes. A stalker can exploit such a device.

Internet Feature of Anonymity

The findings revealed that all respondents agreed that the cloak of anonymity provided by the Internet makes cyberstalking more ideal than real-world stalking. One respondent from a regulatory body stated that:

> The lure of anonymity makes it easy for stalkers to stalk any victim. Anonymity is a factor in the commission of cyberstalking. It makes cyberstalking easier. One could be at one's workplace or home or anywhere to stalk one's victim.

Manufactured Risks and Over-sharing of Personal Information

The findings suggested that the computer users who are victimised by cyberstalkers are manufacturing cyberstalking risks suffered by them. The majority of the respondents suggested that the risk of cyberstalking was manufactured or created by computer users themselves by over-sharing of personal information online or on social media applications. A respondent stated that:

> I think the risk of cyberstalking is what we create ourselves, and it is occurring due to our eagerness to share everything in our life online either on Facebook or Instagram.

Users' Lack of Cyber Security Awareness

The findings revealed that half of the respondents believed that with the advancement of technology and the increase in its usage, computer and mobile users were not equipped with cybersecurity awareness or education in protecting themselves against any cyberstalking. A respondent from an enforcement body stated that:

> Many computer users nowadays have zero awareness or knowledge about cybersecurity. They think that they are safe when putting their personal information online. They did not think that cyberstalkers might use that information.

The Rationales for Non-Criminalisation of Cyberstalking

Law Lags Behind Technology

The findings revealed that most respondents believed that in more than twenty years, the current laws contained in the CMA 1998 has lagged behind technology and were out of date. One respondent stated that:

> The CMA was enacted in 1998 and was enforced in April 1999. The legislators at the time did not foresee crimes like cyberstalking happening.

The Misconception of the Adequacy of Existing Laws

The findings suggested that most respondents misconstrued the adequacy of the current laws in protecting cyberstalking victims. A respondent from a legal firm remarked that:

> Cyberstalking is a crime under the existing law, and similar reliefs are available under the Domestic Violence Act, and under the Rules of Court 2012 and by common law (for example, *quiatimet* injunctions).

Technology as the Solution and Individual Responsibility

The majority of the respondents believed that technology such as password authentication, blocking software and security software rather than the law could be an

effective modality to mitigate the risks of cyberstalking. They also perceived that in such a risk-mitigation exercise, self-regulation, or individual responsibility is paramount. A representative of the Bar Council stated that:

> When we do not have the law to protect us, perhaps it is more effective to block the cyberstalker from our hand phone, Facebook, Instagram and Twitter accounts. Moreover, we need to learn how to self-regulate our online actions and to take care of our online security and safety. If we do not do that, we have ourselves to blame when we are being stalked.

Lack of Political Will and Priority

The findings indicated that most respondents thought that the Government have not given cyberstalking much thought and have lacked the political will to enact any law on it. A respondent observed that:

> In the Malaysian political environment, I don't think the Government is interested nor has the political will to create a new law on cyberstalking. The relevant ministry has its priority on what law they want to establish.

The Impact of Non-Criminalisation on Victims

The findings indicated that some respondents believed that the current laws do not offer much protection to cyberstalking victims as it is a non-specific stalking law and has denied any sense of justice to victims of such crime. A legal practitioner observed that:

> Seriously I don’t see what adequate protection or justice is being afforded to the cyberstalking victims with the kind of law that we have now in the Penal Code and the CMA.

The findings also showed that most respondents were favourable to the creation of a specific law to protect cyberstalking victims such as that in England and Wales, which would guarantee justice is served to cyberstalking victims. A respondent from a regulatory body remarked that:

> Malaysia needs to create a specific cyberstalking law with the kind of legal protection for victims like the one in the UK, which has the necessary court protection orders. We need to establish the anti-cyberstalking law where justice is done or seen to be done to cyberstalking victims.

Discussion

The findings or the narratives of the respondents on the factors contributing to cyberstalking seem to confirm the literature that the drivers and motivations for cyberstalking are diverse, ranging from technological or ICT developments, the commercialisation of the world-wide-web since the early 1990s and the Industry Revolution 4.0 (Reyns, 2015; Storey & Hart, 2011, Wall, 2018; Smoker and March, 2017; Li, 2018, Mueller et al., 2019, Khan & Tan, 2020) to the opportunity configurations (Moon & McClusky, 2010; Aa, 2011; Mutawa, 2016) and the anonymity presented to criminals by the structure of the technology (Aa, 2011; Reyns, 2015; Cheyne & Guggisberg, 2019). The narratives and findings are also in line with Giddens' view of manufactured risk within the Risk Society Theory, which suggests that human factor is significant in understanding the risks involved in using ICT (Beck, 1992; Giddens, 1999). People may unwittingly manufacture their risks of being cyberstalked when they freely share

personal information online (Perry, 2012; Ngo & Paternoster, 2013) but also when computer users are deficient in cybersecurity awareness and education (Hamin & Wan Rosli, 2020).

With regards to the justifications for the non-criminalisation of cyberstalking in Malaysia, the findings confirm the well-known fact that law is perpetually lagging behind technology (Todd, Bryce & Franquire, 2020). Moreover, the findings showed that the preference for a technological solution as opposed to the law when dealing with cyberstalking is in line with recent studies on cybercrimes (O'Shea et al., 2019). Also, the findings revealed that self-regulation or individual responsibility is present, in which computer users need to manage their risks against cyberstalkers and to assume some portion of the blame for their failure to manage such risks. Such a position seems to suggest that such findings are in line with O'Malley's 'privatised prudentialism' (O'Malley, 1999).

The findings on the impact of non-criminalisation on victim's protection and justice to them are in accordance to local legal literature which suggests that the existing legal framework in Malaysia is not adequate to address cyberstalking as it is not expressly or directly addressed under the CMA 1998 (Mifha, Conrad & Gibson, 2019). They further contend that specific legislation should be enacted to govern cyberstalking to ensure that the offenders are duly prosecuted, and the crime is appropriately regulated. Such findings also support the view that there is no specific law which criminalises stalking and harassment even though there are several provisions of law that prohibit specific actions that border on stalking and harassment (Foong, 2018). He further contends that Malaysia should follow the Singaporean counterpart in enacting specific anti-stalking laws to govern stalking and cyberstalking. The recent amendment to the Domestic Violent Act 2017 provides legal protection to victims of domestic violence against the abusive stalkers. However, such protection is only available to victims who are in marital and familial relationships (Hamin & Wan Rosli, 2020).

Conclusion

The findings revealed that the catalysts for cyberstalking are varied and that such crime has not been specifically criminalised in the Malaysian cyber laws or traditional criminal legal frameworks. Despite the increasing number of reported cyberstalking cases, the failure by the Government to take the necessary measures to criminalise stalking is unacceptable. Such a stance does not bode well for cyberstalking victims and a blatant denial of justice to them. Furthermore, the recent legislation which protects stalking victims appears to be discriminatory as such protection is only available to such victims who are in marital and familial relationships. Therefore, such protection is not comprehensive and does not provide the full protection for numerous cyberstalking victims who are outside such a relationship. It is asserted that the existing legal framework, be it the traditional or cyber law, is insufficient to deal with cyberstalking and hence, there is a dire need for an immediate review so that a new law or an amendment to the existing law should be taken to provide adequate protection and justice for the cyberstalking victims. The legal lacuna calls into question not only the adequacy of the current law in dealing with such crime but also the availability of legal protection and the provision of justice for cyberstalking victims as envisaged by the National Cyber Security Policy (NCSP) 2006. Thrust 2 of the NCSP, which relates to the Legislative and Regulatory Framework, declares the need to review and enhance Malaysia's cyber laws to address the dynamic nature of cybersecurity threats. Besides, the Sustainable Development Goals (SDG) No.16 on Peace, Justice and Strong Institutions suggests that the promotion of the rule of law at the national and international level is paramount. However, unless and until

there is a political will to criminalise such crime and to be in accordance with the NCSP and SDG, which would inevitably protect the victims of such crime, the legal future and justice for cyberstalking victims remain ambiguous.

Acknowledgements

This work was supported by research grant FRGS/1/2019/SSI10/UITM/02/2 by the Research Management Centre, UiTM Shah Alam, Selangor.

References

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).

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

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

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.

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.

Fissel, E. R., & Reyns, B. W. (2020). The Aftermath of Cyberstalking: School, Work, Social, and Health Costs of Victimization. *American Journal of Criminal Justice*, *45*(1), 70-87.

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., & Rosli, W. R. W. (2020). Whither the Protection for Cyberstalking Victims? Some Evidence from Malaysia. *Environment–Behaviour Proceedings Journal* 5(S11), 53-58.

Hamin, Z., & Rosli, W. R. W. (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.

Haron, H., Yusof, F. (2010). Cyber Stalking: The Social Impact of Social Networking Technology. *International Conference on Education and Management Technology* (ICEMT 2010).

Heinrich, P., A. (2015). Generation Istalk: An Examination of the Prior Relationship between Victim of Stalking and Offenders, Theses, Dissertations and Capstones, Paper 917.

Kalaitzaki, A. (2020). Cyberstalking Victimization and Perpetration Among Young Adults: Prevalence and Correlates. In *Recent Advances in Digital Media Impacts on Identity, Sexuality, and Relationships* (pp. 22-38). IGI Global.

Khan, S., Khan, N., & Tan, O. (2020, February). Efficiency of Legal and Regulatory Framework in Combating Cybercrime in Malaysia. In *Understanding Digital Industry: Proceedings of the Conference on Managing Digital Industry, Technology and Entrepreneurship (CoMDITE 2019),* July 10-11, 2019, Bandung, Indonesia (p. 333). Routledge.

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

Amanda, M. 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 Decatur St., Atlanta, Georgia 30303 http://gsulaw.gsu.edu/lawand/papers/fa02/medlin/.

Miftha, A., Conrad, M., & Gibson, M. (2019). Cyber Stalking is a Social Evil: From the Indian Women's Perspective. Retrieved online from

https://uobrep.openrepository.com/bitstream/handle/10547/623527/Cyberstalkingisasocialevil.pdf?sequence=2&isAllowed=y

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

O'Shea, B., Julian, R., Prichard, J., & Kelty, S. (2019). *Challenges in Policing Cyberstalking: A Critique of the Stalking Risk Profile in the Context of Online Relationships. In Online Othering* (pp. 331-353). Palgrave Macmillan, Cham.

Papakitsou, V. (2020). Cyberstalking, A New Crime: The Nature of Cyberstalking Victimization. *Dialogues in Clinical Neuroscience & Mental Health*, *3*(3), 197-202.

Reyns, B. W. (2019). Online Pursuit in the Twilight Zone: Cyberstalking Perpetration by College Students. *Victims & Offenders*, *14*(2), 183-198.

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

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

Smoker, M., & March, E. (2017). Predicting Perpetration of Intimate Partner Cyberstalking: Gender and the Dark Tetrad. *Computers in Human Behaviour*, 72, 390-396.

Todd, C., Bryce, J., & Franqueira, V. N. (2020). Technology, Cyberstalking and Domestic Homicide: Informing Prevention and Response Strategies. *Policing and Society*, 1-18.

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