KDU Law Journal
General Sir John Kotelawala Defence University, Sri Lanka

Volume 02, Issue 01
March, 2022

ISSN 2783-8870

Stalking and Cyber Stalking: A Comparative Analysis of the Legislative Responses in Sri Lanka, Canada, the United Kingdom and Australia

Madushan Indrakumara*
Luckmali Fernando**

Abstract

The act of stalking has its own silent effects on victims at times even it could prove fatal. Yet owing to the complex nature of the conduct of stalking, it has evaded the attention of the legislature particularly in Sri Lanka. Through the expansion of the technology, the act of stalking had been updated furthering the impact, yet surprisingly, it still has failed to secure the attention of the legislature. This paper seeks to define and analyze the terms of stalking emphasizing on cyber stalking in the Sri Lankan context. To attain this objective, the Black Letter approach has been utilized together with comparative research methodology, with the United Kingdom, Canada and Australia. Further, this paper uses qualitative analysis of legislative enactments and case law as primary data and books and journal articles as secondary data. This article concludes with the view that Sri Lanka requires legislative intervention to address the real threat of cyber stalking.

Keywords; *Stalking, Cyber stalking, Harassment, Victims, Legislative Response*

*LLM (OUSL reading), LLB (KDU), Attorney at Law.
**MA (Peradeniya), LLB (Deakin, Australia), BA (Deakin, Australia), Dip of Business (Swinburne, Australia), Attorney at Law.

Introduction

The event of cyber stalking can be identified as another extension of criminal conduct of a perpetrator using enhanced electronic capabilities, to attain the end of causing violence against another[1]. The act of stalking has been addressed extensively by other jurisdictions apart from Sri Lanka. Even in those jurisdictions the act of stalking encompasses relatively novel characteristics[2]. Stalking reflects a more trait description similar to shoplifting, hooliganism and vandalism, rather than being categorically confined to a legal matter[3]. In an attempt to gather a more generic meaning for the word 'Stalking', the act of one or the course of repetitive conducts of one, which inflicts intrusion and unsanctioned communication on another, prolonging and persisting to the extent that the recipient of such acts would feel threatened and intimidated[4]. The act of stalking itself is an accumulation of several motive and purposes, which are intrinsic to human behavior and emotions such as jealousy, resentment, obsession and the overwhelming desire to infer control over someone[5]. When characteristics of the victims are concerned, mostly existence of some form of acquaintance is common, such as a former partner or a relative, but the incident occurring between complete strangers are not unusual[6]. Stalking of celebrities and popular figures can be easily elevated into domestic violent encounters[7].

From close observation, the act of stalking can be identified to be manifested through various activities ranging from, following constantly keeping surveillance, to repetitive acts of communications such as texts messages, phone calls and emails to the victim[8]. It may further extend to sending or leaving the victim with offensive materials and sometimes

[1] J. Clough, Principles of Cybercrimes, (1st publication, Cambridge University Press, Cambridge 2010) 365.
[2] The Oxford English Dictionary cites the first example in 1984
[3] C. Wills, 'Stalking: The Criminal Law Response' (1997) Criminal Law Review 463, 463.
[4] R. Purcell, M. Pathe and P. E. Mullen, 'Stalking: Defining and prosecuting a new category of offending' (2004) 27 International Journal of Law and Psychiatry 157,157.
[5] E. Ogilvie, 'Stalking: Legislative, policing and prosecution patterns in Australia', (2000) 34 AIC Research and Public Policy Series 19, 20
[6] A.G. Burgess, J.E. Douglas and R. Halloran, 'Stalking behaviours within domestic violence' (1997) 12 Journal of Family Violence 389.
[7] S. Walby and J. Allen, 'Domestic Violence, Sexual Assault and Stalking: Findings from the British Crime Survey' (2004) Home Office Research Study 276.
[8] P. Tjaden and J. Thoennes, 'Prevalence, Incidence, and Consequences of Violence Against Women: Findings from the National Violence against Women Survey' (1998) US Department of Justice, Office of Justice Programs 10.

Volume 02, Issue 01
March, 2022
ISSN 2783-8870

committing violence against the property of the victim[9]. The consistent occurrence of these acts for a prolonged period of time, from days, months and even years, can be identified in the acts of stalking. It is this persistence that proves a grave psychological threat to the victim even though apparent physical violations are absent[10]. Further these psychological effects of stalking can lead to various adverse impacts resulting in, sleep deprivation, anxiety, depression, suicidal tendencies and post-traumatic stress disorder[11].

The adverse effect and the conduct of stalking is not a novelty in any jurisdiction, yet it still holds a difficult area for prosecutions in absence of a specific offence tailored to suit it[12]. This difficulty is rather more pronounced when proving the threat or fear caused in the absence of actual threatening conduct. Therefore in many jurisdictions, prior to the introduction of anti-stalking legislation, the prosecution had to rely on other possible offences such as offences against the person and property, and other harassment prohibition legislations[13]. The introduction of the offence of stalking is to cater to the gap, for the offence itself relies not on a single act but the impact that one such act could have collectively throughout a passage of time, culminate anxiety and uncertainty in the mind of the victim[14].

Methodology

This paper is relying on the qualitative approach in conducting the research and gathering the required data. As the primary source of data gathering legislative enactment of various jurisdictions such as the United Kingdom, Canada, Australia and Sri Lanka and judgments delivered by the courts of those respective jurisdictions were used,

[9] Emily Finch, The Criminalisation of Stalking: Constructing the Problem and Evaluating the Solution, (1st edn, Routledge-Cavendish, London 2001) 289–305

[10] P. Tjaden and J. Thoennes, 'Prevalence, Incidence, and Consequences of Violence Against Women: Findings from the National Violence against Women Survey' (1998) US Department of Justice, Office of Justice Programs 10.

[11] I.Grant, N.Bone and K.Grant, 'Canada's criminal harassment provisions: A review of the first ten years' (2003) 29 Queen's Law Journal 175, 185–8

[12] J.Clough, Principles of Cybercrimes, (1st publication, Cambridge University Press, Cambridge 2010) 366.

[13] Emily Finch, The Criminalisation of Stalking: Constructing the Problem and Evaluating the Solution, (1st edn, Routledge-Cavendish, London 2001) 119–72

[14] J.Clough, Principles of Cybercrimes, (1st publication, Cambridge University Press, Cambridge 2010) 366.

and from the secondary data gathering books, journal articles and web articles were utilized. The choice of the above jurisdictions was based on the collective advancement of anti-stalking laws in those countries to be stated side with Sri Lankan legislative responses to the similar matter.

Cyber Stalking- The Novel Way of Stalking

The meaning of the word stalking itself is indeed vague with lack of precision, therefore the word of cyber stalking cannot be defined without imprecision. In rather simplistic form it can be identified as the act of stalking conducted through and by the use of technology, such as social media, emails, internet and other such communication enhancements[15]. These communication technological developments tend to facilitate more stalking compared to the offline environment by removing the traditional restraints put between the victim and the offender, it may even facilitate as a direct line of communication that would be impossible for the stalker to establish in an offline environment[16]. The other factor which encourages such behavior is the pseudonymity one can attain on the internet, by this pretence, one who would normally be discouraged to stalk may be encouraged through the safety of the visage to contact the victim and use threatening messages and conduct[17]. This aspect of absence of physical contact may prove to be a further aggravation, by leading the stalker to entertain fantasies and encouraging more narcissistic traits towards the victim, later to manifest into violence, through the humiliation of rejection[18].

To summarize, cyber stalking in a legal context is the prolonged and repeated use of abusive behaviors online (a course of conduct or conduct)

[15] L. Ellison and Y. Akdeniz, 'Cyberstalking: The regulation of harassment on the Internet' (1998) Criminal Law Review, Special Edition in 'Crime, criminal justice and the Internet' 29.
[16] M. McGrath and E. Casey, 'Forensic psychiatry and the Internet: Practical perspectives on sexual predators and obsessional harassers in cyberspace' (2002) 30 Journal of the American Academy of Psychiatry and the Law 81, 85.
[17] L. Ellison, 'Cyberstalking: Tackling harassment on the Internet' in D. S. Wall (ed.), Crime and the Internet (London: Routledge, 2001) 143.
[18] M. McGrath and E. Casey, 'Forensic psychiatry and the Internet: Practical perspectives on sexual predators and obsessional harassers in cyberspace' (2002) 30 Journal of the American Academy of Psychiatry and the Law 81, 85.

Volume 02, Issue 01
March, 2022
ISSN 2783-8870

intended 'to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate[19]'.

Cyber stalking can be categorized as follows and these categories are not exclusive to cyber stalking, these overlap and combine with the traditional form of stalking.1) Establishing communication with the victim.2) Publication of victims' unconsented information 3) Victim's electronic device being targeted 4) Surveilling the victim 5) Ongoing threatening behavior.

Legislative Responses

Cyber stalking proves rather more challenging to govern and regulate than the already complex anti-stalking legislation. When regarding the forms of cyber stalking they prove more complex than traditional stalking but it mirrors similar traits as the latter. Hence by broadly defining traditional stalking, most jurisdictions have incorporated cyber stalking to the same. Thus, the tendency is to couple it under the general offence of stalking. However, difficulties arise when some jurisdictions such as Canada have used narrow definitions and identifies it as a distinct category of its own[20].

Furthermore, in some jurisdictions cyber stalking is counter under the umbrella term of harassment[21]. Though not profound there are other jurisdictions which had demarcated more serious cases of stalking from harassment offences, creating a separate offence[22]. There is a repository of ideas which suggest this method is to be most favored among the rest[23].

In the jurisdiction of Australia, any specific anti-stalking Federal laws

[19] Online Harassment Field Manual, 'Defining "Online Abuse": A Glossary of Terms' <https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/> accessed 25 October 2021.

[20] J.Clough, Principles of Cybercrimes, (1st publication, Cambridge University Press, Cambridge 2010) 375; N. H. Goodno, 'Cyberstalking: A new crime: Evaluating the effectiveness of current state and federal laws' (2007) 72 Missouri Law Review 125

[21] T. McEwan, P. Mullen and R. MacKenzie, 'Anti-stalking legislation in practice: Are we meeting community needs?' (2007) 14 Psychiatry, Psychology and Law 207, 215.

[22] Ibid.

[23] T. McEwan, P. Mullen and R. MacKenzie, 'Anti-stalking legislation in practice: Are we meeting community needs?' (2007) 14 Psychiatry, Psychology and Law 207, 215.

are absent, apart from the law which prohibits the usage of carriages to harass individuals[24]. Yet this gap has been addressed at State levels catering for the offence of stalking[25]. In order to confine this discussion the focus of this paper will be on section 21A of the Crimes Act 1958 (Vic), which gives a ten year maximum sentence[26]. The section makes it an offence when someone engages in a course of conduct having an intention to inflict harm on the victim, mental or physical, or the conduct which arouses fear of safety in the victim or any other person.

When the Canadian jurisdiction is considered, stalking can be identified as conduct that would constitute an offence under the laws on harassment. The Section 264(1) of the Criminal Code criminalizes the conduct of anyone who causes any reasonable man to apprehend a fear of their safety or the safety of anyone known to them, whether the conduct is done intentionally to harass the victim or was reckless about that fact[27]. The interesting fact about the legislation regarding the topic in Canada is that it does not require the conduct to be a course of conduct, merely a single act is sufficient to make one culpable[28].

The United Kingdom through the use of section 1 of the Protection from Harassment Act 1997[29], has described, a course of conduct that would amount to harassment with the intent or in the absence of intent having knowledge that such conduct would amount to harassment. In the same Act through section 4 it sanctions more serious acts of causing fear on one through a course of conduct[30].

It can be seen through this fraction of jurisdictions presented, the unanimous need for the enactment of anti-stalking laws, yet even the more general form of stalking without the involvement of cyber technology, proves to be a complex issue, making it difficult to promulgate specific

[24] Criminal Code Act 1995 (Cth) ss 474.15–474.17 (Crowther v. Sala (2007) 170).
[25] Queensland was the first Australian state to enact specific anti-stalking laws in 1993; see Criminal Code Act 1899 (Qld), s. 359E. Also see Crimes Act 1900 (ACT), s. 35.
[26] Crimes Act 1958 (Vic) s 264(1).
[27] The Canadian provision was introduced in 1993, and carries a maximum penalty of 10 years' imprisonment: Criminal Code s. 264(3)
[28] ***R v. Pastore*** (2005) OJ no 2807.
[29] Protection from Harassment Act 1997, s 1.
[30] Protection from Harassment Act 1997, s 4.

Volume 02, Issue 01
March, 2022
ISSN 2783-8870

legislations[31]. The difficulty is to draft specific legislation to address the issue of stalking without sanctioning the legitimate activities conducted by persons. This hurdle is usually addressed by the legislature by using border terms to define the conduct and basing the fault elements on the impact the act has on the victim[32]. To water down the adverse effects of these legislations on legitimate purposes, such as investigative journalism, defenses have been introduced in many jurisdictions[33].

Elements of Cyber Stalking

From a careful analysis of such legislations, three common ingredients could be differentiated. Those are 1) Conduct Element 2) Fault Element 3) Impact on the Victim.

a. Conduct element

In addressing the element of conduct, two positions prominently taken by legislatures in different jurisdictions can be identified. One approach is to mention the word 'course of conduct' and leave it undefined, similar to the United States federal provisions[34]. In contrast the other manner is to define the 'course of conduct'. In the UK the law is undefined on this point, which had included speech to the definition, and necessity of at least two instances of conduct[35]. This approach can be understood as feasible as it provides the courts with enough flexibility to apply its mind, yet the unspecific nature of the law, regarding the conduct which ought to be or not be criminal, is problematic particularly when one is faced with the choice to determine whether the conduct they are about to do is permitted by criminal law or not[36].

The latter approach of definitely specifying the course of conduct, or in some extreme cases even to list out the conducts, has been taken

[31] J.Clough, Principles of Cybercrimes, (1st publication, Cambridge University Press, Cambridge 2010) 367.
[32] Ibid.
[33] See for example, Protection from Harassment Act 1997 (UK), ss. 1(3) and 4(3), and Crimes Act 1958 (Vic), s. 21A (4).
[34] 18 USC § 2261A(2)
[35] Protection from Harassment Act 1997 (UK), s. 7(3)–(4). Even where there are two incidents, the circumstances must be such that they may properly be described as a 'course of conduct': see Lau v. DPP [2000] EWHC QB 182
[36] J.Clough, Principles of Cybercrimes, (1st publication, Cambridge University Press, Cambridge 2010) 368

as the legislative approach in some jurisdictions[37]. This approach of course narrows the room for the court to interfere flexibly yet it keeps a consistent law. Canada can be taken as an example in this regard. Criminal harassment in Canada specifies the conduct to be 1) Following someone repeatedly from place to place. 2) Repeated direct or indirect communication with someone. 3) Watching the living space or the dwelling house, place of residence, place of work, or other such places. 4) Committing conducts that are threatening to other persons of someone akin to them[38].

b. Fault element

When considering the fault elements, there are two underlining principles various jurisdictions have adopted. One is to consider the importance of the fault element to narrow down an otherwise broad spectrum. Assigning a fault element to a definition such as the intention or recklessness has been the way to comply with this principle. For example, the US Federal rules require the conduct to be intentional to impose sanctions[39]. In Canada the knowledge or the recklessness of the offender should be proved[40]. The other principle of consideration is the acknowledgment of the fact that most of the stalkers do not intend any harm but rather pursue to establish relationships with the target through their misguided methods[41]. Most times they would not even possess the knowledge that the acts they perform do harass the other person[42].

c. Impact on the Victim

This element acts as a limitation on the scope of the offence in many anti-stalking laws. The impact on the victim should at least be sufficient to arouse fear in the victim for their safety. Therefore the provisions which emphasize this element focus more on the impact the conduct makes on the victim rather than the nature of the conduct[43]. This cannot be taken as an objective view, in various jurisdictions this principle has

[37] J.Clough, Principles of Cybercrimes, (1st publication, Cambridge University Press, Cambridge 2010) 368
[38] Criminal Code RSC 1985, c C-46 (Can), s 264(2)
[39] 18 USC § 2261A(2)
[40] Criminal Code RSC 1985, c C-46 (Can), s 264(1)
[41] J.Clough, Principles of Cybercrimes, (1st publication, Cambridge University Press, Cambridge 2010) 368.
[42] I.Grant, N.Bone and K.Grant, 'Canada's criminal harassment provisions: A review of the first ten years' (2003) 29 Queen's Law Journal 175, 185–8.
[43] J.Clough, Principles of Cybercrimes, (1st publication, Cambridge University Press, Cambridge 2010) 374.

Volume 02, Issue 01
March, 2022
ISSN 2783-8870

been adopted subjectively. In the UK, it is a prerequisite to prove that the conduct harassed the victim, and the definition of harassment contains itself the causing of distress or alarm to a person[44]. On the other spectrum of this principle, some jurisdictions have done away with the requirement of an impact on the victim by the conduct, but rather rely on the nature of the conduct itself regardless whether the victim had the knowledge of that particular conduct[45].

Legislative Response in Sri Lanka

In Sri Lanka cyber stalking including cyber harassment has been increasing exponentially over the past few years, preying on countless victims[46]. Most stalkers target vulnerable teenage girls because it is easy to evade criminal penalties as victims in this category are fearful to report due to the social stigma associated and may feel defenseless having minimal recourse from law enforcing bodies.

The officer in charge in Arumapperuma states that 'there are women who are being stalked and harassed by men on different social media accounts. There are complaints of money extortion. Some women do sexual favors as they are threatened[47]'. A recent popular case was the Mt Lavinia child sex trafficking case; some of the offenders committed cybercrimes such as cyber harassing, sharing of obscene material via cyberspace together with crimes committed in a physical level[48]. The plausible reason for the rise in cyber stalking and cyber harassment is that no clear or rigid legislation covers cyber stalking in Sri Lanka. Stalkers and harassers are fearless to commit crimes either because they are unaware that they are committing a crime or due to the relaxed law enforcement mechanism regarding cybercrimes.

[44] Protection from Harassment Act 1997 (UK), s 7(2).

[45] T. McEwan, P. Mullen and R. MacKenzie, 'Anti-stalking legislation in practice: Are we meeting community needs?' (2007) 14 Psychiatry, Psychology and Law 207, 215.

[46] One-Text Initiative, 'Porn and Nudes: Delving into Cyber Exploitation in Sri Lanka' (22 March 2021) <https://onetext.org/index.php/admin/OneText/contents_view/en/Articles/477> accessed 27 October 2021.

[47] Nadia Fazlulhaq, ,'Sri Lanka 'groping in the dark' on how to deal with cyber-bullies',The Sunday Times (Colombo, 7 March 2021) <https://www.sundaytimes.lk/210307/news/sri-lanka-groping-in-the-dark-on-how-to-deal-with-cyber-bullies-434821.html> accessed 27 October 2021

[48] Pavani Hapuarachchi, , '17 arrested in Mt. Lavinia Child sex trafficking ring', NewsFirst (30 June 2021) < https://www.newsfirst.lk/2021/06/30/17-arrested-in-mt-lavinia-child-sex-trafficking-ring/> accessed 26 October 2021.

Unintentionally, the lax laws regarding the crime encourage stalkers to exploit victims boldly.

However, the Computer Crimes Act covers cybercrimes thus one can argue that cyber stalking is dealt within this Act to a limited extent[49]. Sri Lanka was the first South Asian State to assent to the Budapest Convention (the Convention on Cybercrime)[50]. The Computer Crimes Act is largely based on this convention, even though some features such as child pornography are not addressed.

Section 2 of the Computer Crime Act provides broad jurisdiction to include complaints irrespective of whether the person resides, the crime was committed, device or service used, or the loss or damage was caused to a person or corporation, in Sri Lanka or outside Sri Lanka[51]. However the Computer Crimes Act has thus far been interpreted in a narrow scale to substantively include computer related crimes and hacking offences[52], whereas relatively modern Cybercrimes such as that affects one's integrity, well-being or reputation have been vaguely defined. Specific definitions are not provided by any legislation for offences such as cyber stalking, cyber bullying, cyber harassment, hate speech, cyber defamation, cyber-squatting and cyber gambling[53]. Therefore, since the Computer Crimes Act is the primary statute that deals with crimes committed via cyberspace, it can be interpreted to consider crimes such as cyber stalking and cyber harassment as a computer crime. Cyber stalking comes under computer integrity, accessibility and confidentiality of data. Section 7 of the Act categorizes obtaining unlawful data as an offence and section 10 states that unauthorized disclosure of information enabling access to a service is an offence[54]. Attempt to commit an offence under this Act, abetment and conspiracy is dealt with under sections 11, 12, 13 respectively.

[49] Computer Crimes Act No 24 2007.

[50] Damithri Kodithuwakku, 'An evaluation of the legal framework of cyber-crimes in Sri lanka' (2019) Junior BASL 1, 4; Convention on Cybercrime [23 November 2001], available at: <https://www.refworld.org/docid/47fdfb202.html> accessed 28 October 2021.

[51] Computer Crimes Act No 24 2007 s 2.

[52] Jayantha Fernando, 'Cybercrime Legislation – Sri Lankan Update' (2016) COE 1, 2

[53] Damithri Kodithuwakku, 'An evaluation of the legal framework of cyber-crimes in Sri lanka' (2019) Junior BASL 1, 4.

[54] Computer Crimes Act No 24 2007 ss 7, 10

Volume 02, Issue 01
March, 2022
ISSN 2783-8870

These sections can relate to cyber stalking cases. However, these provisions have not been critically analyzed by the judiciary to allow for such extension or inclusion[55]. Therefore, victims of cyber stalking or other non-defined cybercrimes cannot be protected under the Computer Crimes Act due to the lack of knowledge and inadequate interpretations of the law[56]. Offenders and law enforcing bodies may also be ignorant about the law due to its ambiguity. Therefore, though Sri Lanka was progressive in enacting the statute, the implementation and enforcement of the legislation are lagging.

The right to privacy is not provided by law expressly in Sri Lanka. However, Sri Lanka has ratified the International Covenant on Civil and Political Rights (ICCPR) thus is obliged to follow the rights enshrined in the treaty. Article 17 of the ICCPR guarantees the right to privacy[57]. However, the domestic law enacting the ICCPR does not provide for the right to privacy. Article 11 of the Constitution provides for the fundamental right that 'no person shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment[58]'. A case of cyber stalking may be brought under this guaranteed right[59]. However, no case has been brought before the court to comprehend the judiciary's interpretation. Another legislation that may embody cyber harassment is under section 345 of the Penal Code, which is in regards to sexual harassment in a non-cyber platform[60]. Similarly, section 374 of the Penal Code relates to extortion and section 483 relates to criminal intimidation[61]. Furthermore, the Domestic Violence Act, Obscene Publication Ordinance, Child Protection Authority Act, etc. protect individuals from harassment[62]. Thus, it is evident that though there is a multitude of laws that cover sexual harassment, defamation, domestic

[55] Aparrajitha Ariyadasa, 'Harassment Beyond Borders: Sexting, Cyber Bullying and Cyber Stalking in Social Media. Can Sri Lanka Protect Victims?' (2019) Papers SSRN 1, 6.
[56] Ibid.
[57] International Covenant on Civil and Political Rights 1966 art 17; International Covenant On Civil and Political Rights (ICCPR) Act, No. 56 of 2007 (Sri Lanka).
[58] Constitution of the Democratic Socialist Republic of Sri Lanka, art 11.
[59] Aparrajitha Ariyadasa, 'Harassment Beyond Borders: Sexting, Cyber Bullying and Cyber Stalking in Social Media. Can Sri Lanka Protect Victims?' (2019) Papers SSRN 1, 7; Constitution of the Democratic Socialist Republic of Sri Lanka arts 17, 127.
[60] Penal Code (Sri Lanka), s 345.
[61] Penal Code (Sri Lanka), s 374, 483.
[62] Obscene Publications Ordinance, s 2; Prevention of Domestic Violence Act No 34 of 2005; National Child Protection Authority Act (No. 50 of 1998)

violence and abuse, no success has been achieved. This is due to the lack of cases being reported and subsequently, case law not being interpreted before the judiciary and the lack of awareness of the current legislation. Therefore, a novel piece of legislation is optimal that specifically relates to cyber stalking and cyber harassment.

The law enforcing agency in Sri Lanka is the Criminal Investigations Department ('CID') with the Cyber Crimes Division focusing on cybercrimes. According to the Cyber Crimes Division ('CCD') there were more than 1000 cyber bullying cases in 2018[63]. Unfortunately, crimes of cyber stalking reported to the body are almost non-existent due to the lack of an acceptable statute encompassing the area of cyber stalking.

Other enforcement bodies include Sri Lanka's Computer Emergency Readiness Team ('SLCERT'), Information and Communication Technology Agency ('ICTA'), Telecommunication Regulatory Commission, Children and Women's Bureau among others. SLCERT has been an effective body in resolving cyber security and forensic issues. SLCERT collaborates with ICTA to combat cyber-attacks[64]. However, its role in regards to cyber stalking is limited. For example, it is involved in resolving cyber cases in regards to social media platforms such as Facebook in rudimentary ways such as reporting profiles directly to Facebook on behalf of the victim.

Another challenge with the enforcing bodies, is the lack of empathy and sensitivity held to complaints. Victims are not comfortable in sharing their experiences, due to the male dominate law binding authorities. This is reflected in the poor reporting rate to investigating bodies. Also, the absence of secure locations and systems to report cyber-crimes, not protecting the confidentiality of the victim, need for oral evidence in court are some problems with regard to reporting cyber-crimes[65]. Moreover, the mentality of the people of Sri Lanka

[63] Aparrajitha Ariyadasa, 'Harassment Beyond Borders: Sexting, Cyber Bullying and Cyber Stalking in Social Media. Can Sri Lanka Protect Victims?' (2019) Papers SSRN 1,4.
[64] Ibid, 7.
[65] Ashan Dharshana, 'Are the Sri Lankan Cyber-Crime Laws Sufficient to Safeguard it Professionals and the Victims of Cyber-Attacks In Sri Lanka?' (12 January 2020) <https://medium.com/@ashanruwanpathirana/are-the-sri-lankan-cyber-crime-laws-sufficient-to-safeguard-it-professionals-and-the-victims-of-7bfb748ab487 >accessed 28 October 2021.

Volume 02, Issue 01
March, 2022
ISSN 2783-8870

must change, they must admit the fact that cyber stalking has become part of internet culture. By being open to change, it will assist victims in seeking support without fear and shame. Other issues in combating cybercrimes in Sri Lanka are problems of identification, lack of computer forensic expertise to conduct investigations and minimal international support in identifying cyber stalkers.

These challenges can be significantly mitigated by the introduction of the Data Protection Act and cyber defamation laws[66]. Also, by creating awareness of the issue among the public, incorporating advanced technology, monitoring social media, creating strong institutions that ensure implementation of the law and safe and secure reporting, establishing prevention strategies and coping mechanisms for the victims. On a positive note, the Women in Need and the Grassrooted Trust closely works with the Sri Lanka Police Women and Children's Bureau and the CCD to bring in proper mechanisms to tackle sensitive cases when recording cyber harassment[67]. However, stringent laws are mandatory to be enacted at a governmental level for successful progress.

Conclusion

The COVID -19 pandemic has augmented the crisis as more people are utilizing the internet and social media frequently in Sri Lanka. Even though, the offences are proscribed by law, no legislation directly discusses these crimes committed via cyber platforms. Therefore, this proposition can be altered if new cases come up before the judiciary and are interpreted in favor of the Computer Crimes Act and other existing legislation or alternatively, a new piece of legislation can be enacted which specifically deals with cyber stalking which details the protections, punishments, enforcement mechanisms and penalties. Sri Lanka must learn from the successful experiences of countries such as the UK, Canada and Australia and adopt a new and thorough legislation that will effectively combat cyber stalking and fill the void in regards to the law.

[66] Asha H Mendis, 'Seeker Are You Protected? Social Media and Protection Granted to Women in Sri Lanka' (2019) 20(7) Journal of International Women's Studies 319, 330.
[67] One-Text Initiative, 'Porn and Nudes: Delving into Cyber Exploitation in Sri Lanka' (22 March 2021) <https://onetext.org/index.php/admin/OneText/contents_view/en/Articles/477> accessed 26 October 2021.