Akademika 96(1), April 2026
https://doi.org/10.17576/akad-2026-9601-04

Assessing Legal Protections against Cyberstalking: A Comparative Analysis of Malaysia, Singapore, Indonesia, and India

Menilai Perlindungan Undang-Undang terhadap Hendapan Siber: Satu Analisis Perbandingan antara Malaysia, Singapura, Indonesia dan India

SAMINA KHAN*, ROHAIDA NORDIN, & MUHAMAD SAYUTI HASSAN

Received: 8-3-2025 /Accepted: 28-5-2026

ABSTRACT

Cyberstalking, characterized by persistent and harmful online behaviours, remains a significant challenge globally. While various jurisdictions have enacted legal frameworks to address cyberstalking, the adequacy and effectiveness of these laws vary across countries. This paper provides a comparative analysis of cyberstalking laws in Malaysia, Singapore, Indonesia, and India, highlighting legal protections, enforcement challenges, and policy gaps. Employing doctrinal legal research and qualitative methods, the study examines statutory provisions and enforcement mechanisms across these jurisdictions. Additionally, the insights from ten semi-structured interviews with legal practitioners, policymakers, and law enforcement officials provide a deeper understanding of how cyberstalking laws operate in practice, with India included as a case study. The findings reveal significant disparities in legal protections, with Singapore's Protection from Harassment Act, 2014, offering one of the most comprehensive frameworks, while Indonesia lacks dedicated legislation on cyberstalking. In Malaysia and India, recent legal developments have criminalized cyberstalking; however, enforcement gaps and limited access to victim protection measures persist. The study highlights the need for harmonized regional policies, improved enforcement mechanisms, and stronger victim-centric legal reforms across Southeast Asia. By identifying key challenges and best practices, this research contributes to the ongoing discourse on strengthening legal responses to cyberstalking in the region.

Keywords: Cyberstalking; legal frameworks; comparative analysis; victim protection; Southeast Asia

ABSTRAK

Cyberstalking, yang dicirikan oleh tingkah laku dalam talian yang berterusan dan berbahaya, terus menjadi cabaran global yang ketara. Walaupun pelbagai bidang kuasa telah menggubal rangka kerja perundangan untuk menangani cyberstalking, kecukupan dan keberkesanan undang-undang ini berbeza di antara negara. Kajian ini menyediakan analisis perbandingan undang-undang cyberstalking di Malaysia, Singapura, Indonesia, dan India, dengan menekankan perlindungan undang-undang, cabaran penguatkuasaan, dan jurang dasar. Dengan menggunakan kajian doktrinal undang-undang dan kaedah kualitatif, kajian ini meneliti peruntukan statutori dan mekanisme penguatkuasaan di negara-negara tersebut. Selain itu, pandangan mendalam daripada sepuluh temu bual separa berstruktur dengan pengamal undang-undang, pembuat dasar, dan pegawai penguatkuasaan undang-undang memberikan pemahaman yang lebih mendalam tentang bagaimana undang-undang cyberstalking beroperasi dalam amalan, dengan India turut disertakan sebagai kajian kes. Hasil kajian menunjukkan perbezaan ketara dalam perlindungan undang-undang, di mana Akta Perlindungan Daripada Gangguan, 2014 di Singapura menawarkan salah satu rangka kerja paling komprehensif, manakala Indonesia masih kekurangan undang-undang khusus mengenai cyberstalking. Di Malaysia dan India, perkembangan undang-undang terkini telah mengkriminalisasikan cyberstalking; bagaimanapun, jurang dalam penguatkuasaan dan akses terhad kepada langkah perlindungan mangsa masih wujud. Kajian ini menekankan keperluan untuk dasar serantau yang diselaraskan, mekanisme penguatkuasaan yang lebih baik, dan reformasi undang-undang yang lebih berpusat kepada mangsa di Asia Tenggara. Dengan mengenal pasti cabaran utama dan amalan terbaik, penyelidikan ini menyumbang kepada perbincangan berterusan mengenai pengukuhan tindak balas undang-undang terhadap cyberstalking di rantau ini.

Kata kunci: Cyberstalking; rangka kerja perundangan; analisis perbandingan; perlindungan mangsa; Asia Tenggara

INTRODUCTION

The advent of technology in the current digital era has led to the emergence of new forms of online crimes, such as online harassment, cyberstalking, and cyberbullying, which are carried out using a variety of information and communication technologies (ICT). These cybercrimes create serious legal and regulatory concerns that affect the larger political and economic environment and pose serious social and psychological difficulties. The evolving nature of these offences puts pressure on the current legal systems and calls for a review of established legal principles to adequately handle the complexity of criminal activity in the digital sphere. It was estimated that around 67 percent of the world's population were internet users in 2023. This marks a significant growth of 45 percent since 2018, during which approximately 1.7 billion new users gained internet access (International Telecommunication Union [ITU], 2023).

The surge in ICT has given rise to hybrid crimes, offences that leverage the internet to enhance traditional criminal activities (Khadim et al., 2022). These hybrid crimes, such as cyberstalking and cyber harassment, can occur both online and offline, with their impact intensified by technology. For instance, cyberstalking can easily extend from the digital realm into real life, demonstrating the interconnected nature of these offences. In today's digital age, traditional crimes are increasingly enabled by technology. While complex offline criminal activities often rely on computers and networks, these digital tools serve as supportive elements rather than being essential to the crimes (Nicola, 2022).

In the global context, existing research on stalking and cyberstalking reveals emerging trends and characteristics. Notably, younger individuals are increasingly at risk of becoming victims of stalking compared to older people (Chan & Sheridan, 2019; Humboldt et al., 2022; Brooks et al., 2021). Stalking is widely recognized as a significant issue with severe social, psychological, medical, and economic consequences (Boehnlein et al., 2020; Dhir et al., 2021; Storey et al., 2023). However, research on cyberstalking is less extensive compared to traditional stalking and remains relatively limited (Abu-Ulbeh et al., 2021; Fissel, 2021; Kaur et al., 2021; Stevens et al., 2021). Over the past years, there has been a major progression in the study of cyberstalking (Ho & Luong, 2022). Studies from the past as well as the present show that cyberstalkers use technology to hide their identities and take advantage of the anonymity provided by the internet to quickly target victims without having to contact them in person (Chang, 2020; Asante & Feng, 2021).

Current legal research on cyberstalking examines the effects and impacts of anti-stalking legislation. Cyberstalking is now illegal in many countries worldwide, with California setting the precedent in 1992. In 1997, the Protection from Harassment Act was passed in the United Kingdom (UK), and the Harassment Act was passed in New Zealand. These laws addressed both civil and criminal harassment. By making cyberstalking an offence in 2014 with the passage of the Protection from Harassment Act, Singapore followed the UK's lead (Rosli et al., 2021). Protection orders, injunctions, damages, and restraining orders are just a few of the ways that victims of stalking can be protected under anti-stalking legislation in the US, Singapore, and the UK (Rosli et al., 2022).

While Southeast Asian countries such as Malaysia, Singapore, and Indonesia have introduced legal provisions addressing cyberstalking, India presents a unique case where both traditional criminal law and cyber law are invoked to address the issue. The Bharatiya Nyaya Sanhita (BNS, 2023), replacing Section 354D of the Indian Penal Code, criminalizes repeated online contact, digital surveillance, and unwanted interaction. However, India lacks

comprehensive civil remedies, such as protection orders, which are available in jurisdictions like Singapore and Malaysia (Rachna & Varshney, 2024). Studies indicate that underreporting remains a significant challenge in India, particularly for female victims of cyberstalking, due to social stigma and law enforcement barriers (Khan et al., 2023).

Data from the National Crime Records Bureau (NCRB) highlights the increasing prevalence of cyberstalking in India. In 2020 alone, 50,035 cybercrime cases were recorded, including 1,614 cases of cyberstalking, 762 cases of cyber blackmail, 84 cases of defamation, 247 cases of false profiles, and 838 cases of fake news. Cybercrime rates rose by 63.48% between 2018 and 2019 and further increased by 12.32% between 2019 and 2020 (Kaur & Saini, 2023). While India has made progress in criminalizing cyberstalking, research on the perception of cyberstalking and the adequacy of existing laws remains limited.

In order to fill this gap, this study examines societal and legal perspectives on cyberstalking across Southeast Asia, with India as a reference point. The paper evaluates the adequacy of cyberstalking legislation in Malaysia, Singapore, Indonesia, and India and explores lessons that can be learned from regional best practices. By conducting a comparative legal analysis and incorporating qualitative insights from law enforcement, legal practitioners, policymakers, and civil society actors, the study seeks to identify existing gaps and propose legal reforms to enhance protections against cyberstalking in Southeast Asia.

LITERATURE REVIEW

Technology's emergence and widespread use have facilitated various activities, including sharing images and information, instant messaging, and engagement on social media platforms (Shanmugasundaram & Tamilarasu, 2023). While these technological advancements have contributed to global connectivity, they have also significantly increased the prevalence of online harassment and stalking (Rao, 2022). Initially, stalking was conceptualized as a crime characterized by persistent, intimidating, and potentially dangerous pursuit behaviors that threaten the victim's safety (Parkhill et al., 2022). However, with the increasing integration of technology into everyday interactions, cyberstalking has emerged as a distinct and pervasive form of digital harassment (Asante & Feng, 2021).

Cyberstalking extends traditional stalking into the online domain, where perpetrators leverage internet-connected devices and digital platforms to monitor, harass, or intimidate victims. The literature highlights the evolution of cyberstalking through two key aspects: the technological mediums used and the variety of illegal activities involved. These activities include unsolicited email communication, chat rooms, mobile applications, SMS, social media, and online forums. Stalking can manifest through repeated malicious disclosure of personal information, issuing threats, or, in severe cases, coercing individuals into harmful interactions (Geldenhuys, 2024). Stevens et al. (2021) define cyberstalking as the persistent and repeated harassment of an individual through online platforms or digital means. Asante and Feng (2021) argue that technological advancements have normalized cyberstalking, fueled by unrestricted digital access, the anonymity of online interactions, and the expansion of communication networks.

Scholars emphasize that the internet offers cyberstalkers opportunities to easily target multiple victims while concealing their identities. Rachna and Varshney (2024) argue that the anonymity provided by online spaces enables perpetrators to conduct widespread surveillance and harassment across jurisdictions. Cyberstalkers can exploit online databases, search engines, and

social media platforms to gather information about their victims, facilitating transnational cyberstalking cases (Stevens et al., 2021). These dynamics present significant jurisdictional challenges, as cyberstalking offenses often involve perpetrators and victims in different states or countries, complicating law enforcement responses (Fissel et al., 2024). This is relevant in Southeast Asia, where cross-border cybercrimes are increasing, and legal frameworks differ widely between jurisdictions.

The literature increasingly recognizes cyberstalking as a transnational crime that requires coordinated legal responses. Rao (2022) highlights that cyberstalking transcends geographical barriers, allowing perpetrators to harass victims remotely, often with little fear of prosecution. Previous qualitative studies have explored various aspects of cyberstalking, including the role of technology in intimate partner stalking (Kim & Ferraresso, 2023), the influence of social network platforms on cyberstalking incidents (Geldenhuys, 2024), and the analysis of cyberstalking legislation in the United States (Rapisarda & Kras, 2023), the UK (Al-Rajhi, 2024) and Singapore (Rosli et al., 2021). Singapore's Protection from Harassment Act (2014) has been noted for its comprehensive scope, providing both civil and criminal remedies, including expedited protection orders. In contrast, Malaysia only recently introduced Section 507A of the Penal Code (2023) to criminalize stalking, including digital harassment. Meanwhile, Indonesia lacks specific cyberstalking provisions, relying instead on general provisions under the Electronic Information and Transactions (EIT) Law (2008). India's legal framework, particularly Section 78 of the Bharatiya Nyaya Sanhita (BNS) and provisions under the Information Technology Act (2000), offers protections but faces enforcement challenges.

Existing literature acknowledges that cyberstalking surpasses traditional stalking regarding reach, impact, and anonymity. The digital nature of these crimes enables perpetrators to conceal their identities, alter or delete critical data, and evade accountability with relative ease (Abu-Ulbeh et al., 2021). Martellozzo et al. (2022) reported that during the 2020 COVID-19 lockdowns, stalking and harassment cases in the UK increased by 20%, further escalating to 31% as restrictions eased, underscoring how reliance on digital platforms has heightened cyberstalking risks globally. While studies highlight the severity of cyberstalking in Western jurisdictions, research on cyberstalking laws and enforcement in Southeast Asia remains limited, pointing to a gap that this study seeks to address.

MULTIFACETED RISKS OF CYBERSTALKING VICTIMIZATION

The various dimensions of victimization associated with cyberstalking have been extensively examined in existing literature. Todd et al. (2020) highlight that victims face physical threats, as cyberstalkers can exploit digital footprints to track locations, potentially leading to physical harm or even lethal outcomes. Additionally, cyberstalkers can uncover personal contact details, including those of the victim's family and friends, posing risks to their privacy and safety. By employing social engineering tactics, they may gather sensitive information to manipulate or deceive victims. Fissel et al. (2024) further note that cyberstalkers often misuse such data to gain access to victims' personal information, which can result in identity theft or exploitation through third parties. Moreover, cyberstalkers may take control of victims' accounts to perpetrate financial and emotional harm, such as accessing bank accounts or sending fraudulent communications. The availability of inexpensive or free spyware increases these risks by enabling cyberstalkers to monitor and collect information about their victims easily (Bailey et al., 2024).

THE RISK SOCIETY IN THE DIGITAL AGE

The concept of a risk society, as articulated by Giddens (1990) and Beck (1992), refers to a society preoccupied with future uncertainties and safety. This focus arises from the hazards and insecurities brought about by societal changes. Technological advancements and shifts in social structures mark these changes. It introduces new risks distinct from traditional, external risks like natural disasters. These new risks, termed 'manufactured risks,' arise from human activities, such as pollution and crime. The evolution of the risk society into a world risk society highlights the globalized and interconnected nature of these risks, including cybercrime, identity theft, and cyberstalking. Despite technological progress, Beck (1992) argues that such advancements paradoxically amplify, rather than mitigate, these risks. The pervasive nature of cyber risks, enabled by the anonymity and global reach of technology, has rendered risk control increasingly challenging globally (Castells et al., 2002).

Mitigating these risks requires proactive measures, such as adopting technological safeguards and fostering greater awareness, as the virtual environment allows perpetrators to exploit anonymity. The shift towards online interactions and minimizing physical boundaries through technological developments have further heightened vulnerabilities to human-made risks, highlighting the urgent need for effective legal and technological responses (Giddens, 1999).

METHODOLOGY

This study employs doctrinal legal research to examine the legal frameworks governing cyberstalking in Malaysia, Singapore, Indonesia, and India. The research focuses on legislative provisions and statutory frameworks, analyzing how different jurisdictions define and regulate cyberstalking within their respective legal systems. Further, a comparative legal analysis was conducted to examine cyberstalking laws across the selected jurisdictions. The research systematically reviewed primary legal sources, including Malaysia's Section 507A of the Penal Code (2023), Singapore's Protection from Harassment Act (2014), Indonesia's Electronic Information and Transactions (EIT) Law (2008), and India's Bharatiya Nyaya Sanhita (BNS, 2023) and Information Technology Act (2000). These statutes were analyzed to assess the legal recognition of cyberstalking, the scope of protections afforded to victims, and the applicability of existing legal provisions. Secondary sources such as academic literature, legal commentaries, and judicial rulings were also reviewed to contextualize the development and effectiveness of these laws.

To complement the legal analysis, qualitative research was conducted to explore expert perspectives on cyberstalking laws, particularly in the Indian context. Semi-structured interviews were carried out with ten key respondents, including legal practitioners, law enforcement officials, policymakers, NGO representatives, and survivors of cyberstalking. These interviews provided insights into the legal challenges victims face, the strengths and limitations of existing legal frameworks, and the need for legislative reform. Respondents were selected based on a purposive sampling approach, ensuring that participants had direct expertise or lived experiences relevant to cyberstalking laws. By focusing on experts with specialized knowledge, purposive sampling facilitated targeted data collection from specific stakeholders whose professional experiences and insights are critical to understanding the effectiveness of the current legal framework (Campbell et al., 2020).

The interview data was analyzed using Atlas. ti (Version 24.1.0), employing a thematic approach to identify patterns in respondents' perspectives. The coding process was deductive and inductive, with predefined themes established based on the research objectives, while additional themes emerged during the analysis. The dual coding approach, integrating both deductive and inductive methods, facilitated a thorough analysis of the data, enabling a deeper and more refined interpretation of participants' perceptions and experiences (Deterding & Waters, 2021). Direct quotations from respondents were incorporated into the findings to enhance the accuracy of interpretation and ensure that diverse perspectives were represented (Glazier et al., 2021). Ethical diligence was upheld throughout the study. Confidentiality was maintained, and all data were securely stored to protect the participants' privacy. By fostering an open and respectful dialogue, the study ensured that the respondents' voices were authentically represented while adhering to ethical research standards.

While the legal analysis covered Malaysia, Singapore, Indonesia, and India, qualitative research was conducted solely on India, serving as a case study to examine how legal provisions operate in practice. The findings from India were contextualized within the broader Southeast Asian legal landscape, allowing for a cross-jurisdictional analysis of legislative effectiveness. By integrating comparative legal analysis and qualitative research, this study offers a detailed examination of cyberstalking laws in Southeast Asia while providing empirical insights into the legal challenges faced by victims in India. The research aims to contribute to ongoing discussions on legislative improvements and harmonized legal responses to cyberstalking across jurisdictions.

LEGAL FRAMEWORK GOVERNING CYBERSTALKING IN MALAYSIA, SINGAPORE, AND INDIA

Cyberstalking laws vary significantly across jurisdictions, reflecting different legal traditions, policy priorities, and enforcement mechanisms. While some countries have enacted specific legislation to criminalize cyberstalking, others rely on broader legal provisions to address online harassment. This section examines the legal frameworks governing cyberstalking in Malaysia, Singapore, Indonesia, and India, highlighting key legislative developments, enforcement challenges, and the availability of victim protection measures. Understanding these differences is essential for assessing the effectiveness of current legal responses and identifying potential areas for reform.

MALAYSIA'S LEGAL FRAMEWORK

Before 2023, Malaysia lacked specific legislation addressing stalking behaviors, including cyberstalking. Victims had to rely on general provisions within the Penal Code and other related laws to seek redress for harassment or intimidation (Rosli et al., 2021). For instance, Section 509 of the Penal Code criminalized words or gestures intended to insult the modesty of a person, while Section 507 addressed criminal intimidation through anonymous communication. However, these provisions were not tailored to address the persistent nature of stalking behaviours, particularly those facilitated by digital means (Hamin, 2023).

Recognizing the legislative gap and the increasing prevalence of stalking incidents, Malaysia introduced significant legal reforms in 2023 (Women's Aid Organisation, 2023). A notable development was the enactment of Section 507A of the Penal Code, which explicitly

criminalizes stalking activities. This section defines stalking as engaging in repeated acts of harassment, intending to cause, or knowing or having reason to believe that such acts are likely to cause distress, fear, or alarm to any person regarding their safety. The law enumerates specific behaviors that constitute stalking, including:

> "following a person in any manner or by any means, communicating or attempting to communicate with a person in any manner or by any means, loitering at the place of residence or business of a person, and giving or sending anything to a person in any manner or by any means."

Importantly, the statute specifies that such acts must occur on at least two occasions to qualify as stalking. Offenders may face imprisonment for up to three years, a fine, or both upon conviction.

In tandem with the Penal Code amendment, the Criminal Procedure Code was also revised to bolster protections for stalking victims. The amendments introduced provisions for protection orders, enabling victims to seek legal intervention to prevent the escalation of stalking behaviors (Women's Aid Organisation, 2023). These protection orders serve as a proactive measure, allowing the court to impose restrictions on the alleged stalker, thereby safeguarding the victim's well-being. These legislative advancements position Malaysia as a progressive jurisdiction in addressing stalking, including cyberstalking. By enacting specific laws that criminalize stalking behaviours and providing mechanisms for victim protection, Malaysia has strengthened its legal framework to combat harassment in both physical and digital realms.

SINGAPORE'S LEGAL FRAMEWORK

Singapore's Protection from Harassment Act (PHA) 2014 serves as a comprehensive legal framework addressing various forms of harassment, including stalking behaviors that occur both offline and online. Section 7 of the PHA specifically criminalizes "unlawful stalking," encompassing actions such as repeated unwanted communication, surveillance, and threats. Although the Act does not explicitly define "cyberstalking," its broad language ensures that online harassment is effectively covered within its provisions (Harasgama & Munasinghe, 2021). The law characterizes unlawful stalking as a pattern of conduct that causes harassment, alarm, or distress to the victim. This includes actions such as following, contacting, or attempting to contact the victim, loitering near their residence or place of work, and any other behaviour that could reasonably be expected to cause distress (PHA, 2014). Individuals found guilty of unlawful stalking under Section 7 face penalties that may include a fine not exceeding $5,000, imprisonment for a term not exceeding 12 months, or both.

Victims of harassment in Singapore have the legal right to seek Protection Orders (POs) and Expedited Protection Orders (EPOs) under the PHA (Ministry of Law Singapore, 2021). These orders prevent further harassment by prohibiting the harasser from continuing their behaviour. A PO is a court order that restrains the harasser from engaging in specified acts of harassment towards the victim. The court may also order the harasser to refrain from communicating with the victim or to stay away from certain locations frequented by the victim. In urgent situations with an imminent risk of harm, victims can apply for an EPO, which can be issued within 24 hours (Yong, 2024). This swift legal remedy ensures immediate protection while the application for a standard PO is processed.

Obtaining a PO or EPO involves applying with the Protection from Harassment Court (PHC), a specialized court established to handle such cases. Applicants must provide evidence of the harassment, such as messages, emails, or witness testimonies, to support their claims. The PHC aims to streamline proceedings to ensure timely and effective victim protection. The PHA is designed to protect all individuals, regardless of gender, and focuses on the impact of the harasser's conduct on the victim rather than the specific nature of the acts (Law Library of Congress, 2019).

Beyond criminal penalties, the PHA allows victims to pursue civil remedies, including suing the harasser for damages resulting from the harassment. Additionally, the court may direct parties involved in harassment disputes to attend counseling or mediation sessions as part of the resolution process, promoting restorative justice and addressing underlying issues (PHA, 2014). Singapore's robust legal framework under the PHA reflects a comprehensive approach to combating harassment and stalking, including cyberstalking. By encompassing a wide range of harassing behaviours and providing accessible legal remedies, the Act ensures that victims have the necessary tools to seek protection and justice.

INDONESIA'S LEGAL FRAMEWORK

Indonesia's legal framework currently lacks specific legislation addressing cyberstalking. Instead, the country relies on Law No. 11 of 2008 on Electronic Information and Transactions (EIT Law) to address certain forms of online harassment. This law criminalizes the transmission of electronic information or documents that contain threats, defamation, or immorality, which can encompass some aspects of cyberstalking. However, the EIT Law does not explicitly define or address cyberstalking, leading to challenges in enforcement and legal interpretation (Permatasari & Pujiyono, 2024).

Enforcement of the EIT Law in cases of cyberstalking has been inconsistent, partly due to ambiguous legal definitions and limited judicial precedents. The lack of specific provisions targeting cyberstalking behaviours makes it difficult for law enforcement agencies and the judiciary to effectively address such cases. Additionally, Indonesia does not offer specific legal remedies, such as protection orders, to safeguard victims of cyberstalking (Sari & Suryani, 2023). This absence of preventive legal measures hinders victims' ability to seek immediate protection against their harassers.

Recognizing these legal gaps, there have been discussions and studies advocating for more comprehensive regulations to address cyberstalking in Indonesia (Sihotang & Sihotang, 2023). Proposals include the inclusion of preparatory criminal acts in the Draft Criminal Code, which could encompass cyberstalking behaviours and provide clearer legal grounds for prosecution. However, as of now, these proposals have not been enacted into law, leaving a significant gap in the legal protection available to victims of cyberstalking in Indonesia.

INDIA'S LEGAL FRAMEWORK

In the current Indian legal framework, cyberstalking is governed primarily by the Bharatiya Nyaya Sanhita, 2023 (hereinafter BNS) and the Information Technology Act, 2000 (hereinafter IT Act). Section 78 of the BNS explicitly addresses stalking, including acts committed via online mediums. Under Section 78(1)(ii), " the use by a woman of the internet, email, or any other form of electronic communication constitutes the offence of stalking." The section provides exceptions where such

conduct is pursued for preventing or detecting crime, under legal authority, or in circumstances deemed reasonable and justified.

The penalties for stalking under Section 78(2) are stringent: "first-time offenders may face imprisonment for up to three years and a fine, while repeat offenders may face imprisonment for up to five years and a fine." Including electronic communication in the statutory definition marks a progressive step towards explicitly addressing cyberstalking. The IT Act, enacted in response to the United Nations Model Law on Electronic Commerce, focuses primarily on regulating commercial aspects of cyber activity and fails to address the non-commercial, criminal nature of cyberstalking. While Section 66A of the IT Act was previously invoked to govern offensive communication, it was later repealed in the case of Shreya Singhal v. Union of India (2015), leaving a void in addressing the misuse of electronic communication for harassment. Furthermore, Section 72 of the IT Act, which penalizes the breach of confidentiality and privacy, provides only a limited remedy and does not comprehensively address the various forms of cyberstalking.

However, the law's effectiveness is hindered by systemic issues such as weak enforcement, corruption, and delays in police action. Its gender-specific language limits protection to women, excluding male victims. Additionally, the law lacks clarity on handling cross-border cyberstalking and foreign offenders, leaving significant gaps in addressing extraterritorial digital offences and classifying cyberstalking as a tort.

The enforcement mechanisms under Indian law also face practical challenges, as evident in cases such as the Palanisamy v. State of Tamil Nadu (2017), where delayed police action and outdated cybercrime technology impeded justice. Issues such as bribery, political influence, and lack of sensitivity in handling cyberstalking complaints further exacerbate the problem. Additionally, the absence of a provision similar to restraining orders or victim protection measures under Indian law leaves survivors vulnerable to continued harassment. The need for legislative clarity is further highlighted by the rapid evolution of technology and social media platforms, which facilitate access to sensitive personal information.

A CASE STUDY OF STAKEHOLDER'S INSIGHTS IN INDIA

While India has established legal provisions to criminalize cyberstalking, the practical enforcement of these laws remains inconsistent. This section presents qualitative insights from interviews with key stakeholders, including law enforcement officials, legal practitioners, policymakers, and NGO representatives, on the challenges and gaps in India's cyberstalking response.

FINDINGS

Role of victim behaviour in cyberstalking risks. The research findings indicate that cyberstalking is largely perceived as a risk that must be managed rather than a crime warranting punishment. Respondents frequently attributed this perception to the rapid growth of communication technologies and the increasing reliance on digital platforms. One respondent noted: "With more people relying on WhatsApp, Instagram, and other social media platforms for everyday communication, the opportunities for misuse have naturally increased." Another highlighted: "Earlier, stalking involved physical presence. Now, with just a mobile phone and an internet connection, someone can harass you without leaving their home." Additionally, many respondents

believed that victims might unintentionally contribute to the risks of cyberstalking due to their online behaviours. For instance, one respondent stated: "When individuals create social media profiles and post personal updates publicly, they are opening doors for potential misuse." Another commented: "The more people connect online, the more chances there are for some to use the internet for their harmful intentions."

A prominent theme emerged was the role of oversharing personal information in intensifying the risks of cyberstalking. Respondents frequently emphasized the need for caution when disclosing personal details on social media platforms. One participant remarked, "People often share every detail of their lives online, but they don't realize how dangerous that can be." Another respondent emphasized: "If you share too much online…like your location or private photos…you're making yourself vulnerable. It's better to be careful about what you post."

These findings highlight that cyberstalking risks are deeply connected to technological advances and user behaviour. While technology has created new avenues for communication, it has also increased the potential for misuse. Respondents stressed the importance of promoting responsible online practices and educating users about the consequences of oversharing to reduce vulnerability to cyberstalking.

Cyberstalking as a gender-inclusive crime. The findings highlighted that most respondents believed cyberstalking is not a crime perpetrated exclusively by men. Both men and women were perceived as potential cyberstalkers, reflecting the gender-neutral nature of technology and online platforms. One respondent from a regulatory body stated: "Cyberstalking is not confined to any one gender. Technology does not discriminate…both men and women have the means to misuse it."

Respondents supported this perspective, highlighting the near-equal participation of men and women in India's digital landscape. A legal practitioner remarked, "Men and women in India now have almost equal access to the internet, so it's wrong to think only men are behind cyberstalking. Anyone with bad intentions can misuse these platforms."
Another respondent highlighted that gender parity in internet usage plays a significant role in shaping this perception, stating: "In India, more women are getting online, and as their digital presence grows, so does the chance of misuse…no matter the gender."

The respondents acknowledged that societal stereotypes often label men as the main perpetrators. However, the anonymity and accessibility of technology allow individuals of any gender to engage in such behaviour. They underlined the importance of addressing cyberstalking as a universal issue rather than one limited to specific demographics.

Perceptions of legal adequacy in addressing cyberstalking. The findings revealed contrasting perspectives on the adequacy of legal frameworks addressing cyberstalking in India. Some respondents expressed confidence in the sufficiency of existing laws, emphasizing that cyberstalking could be addressed through provisions in current legislation. A legal practitioner remarked: "Cyberstalking is addressed under Section 78 of the BNS Act, along with relevant provisions of the IT Act. Victims can also seek remedies through injunctions and other relief measures granted by courts."

Similarly, a respondent from a regulatory authority emphasized the comprehensiveness of the legal system, stating: "India has a robust framework, including the IT and the BNS Act, which deal with harassment and stalking. These laws are sufficient in many cases if properly implemented." However, other respondents believed that existing laws, while helpful, lacked the

specificity and depth needed to address cyberstalking. They pointed out that gaps in implementation and the absence of targeted provisions made it challenging for victims to seek justice effectively. A respondent noted:

> "The IT Act is outdated when it comes to addressing technology-facilitated crimes like cyberstalking. There's a need for dedicated legislation that addresses the intricacies of online harassment, just like we've seen in other countries."

Several respondents highlighted the importance of learning from international frameworks. A respondent suggested:

> "India should consider adopting a specific anti-stalking law similar to what we see in countries like the UK or Australia. These laws provide comprehensive protections and address the unique challenges faced by victims in the digital age."

The findings emphasized the necessity of bridging the gap between the existing laws and the dynamic nature of cybercrimes. While Indian lawmakers' efforts are recognized, the respondents emphasized that creating a focused and victim-centered legislative framework would provide more clarity and support to those affected by cyberstalking. This would ensure a stronger alignment with global standards and better protection for victims in the evolving technological landscape.

Mitigating cyberstalking risks. The findings highlighted that respondents believed cyberstalking risks must be regulated to ensure online safety. They proposed several approaches to address these risks, including reporting complaints, using digital tools and techniques to prevent, mitigate, or respond to cyberstalking incidents, and promoting awareness campaigns.

Reporting to the police. A significant number of respondents emphasized the importance of reporting cyberstalking incidents to law enforcement authorities. Lodging a police complaint was seen as an essential step in addressing and documenting such crimes. A respondent noted:

> "We always encourage victims to file complaints with the cybercrime unit at their nearest police station. Providing relevant details, such as screenshots and chats, is very important for the investigation."

Another respondent from a regulatory agency stressed that a systematic complaint mechanism ensures that cases are officially recorded and increases accountability. They stated: "Filing a report not only helps track the perpetrator but also strengthens the need for stricter enforcement of cyber laws."

Using technology to mitigate risks. Respondents also suggested that technology can play a pivotal role in minimizing cyberstalking risks. Measures such as password protection, blocking and reporting stalkers, and utilizing robust security software were highlighted as effective strategies. One respondent explained: "Simple steps like using strong passwords and immediately blocking suspicious accounts on social media platforms can significantly reduce such incidents to happen." Additionally, there was a call for greater awareness among users about online security tools. A respondent remarked: "People often overlook basic precautions while using the internet. Tools like firewall protections and anti-spyware software are easily available, yet many users don't prioritize their use."

Awareness and collaborative efforts. A key strategy identified by respondents was the need for widespread awareness campaigns and educational initiatives. These campaigns, led by government agencies, NGOs, and educational institutions, were seen as critical to sensitizing the public about the risks of cyberstalking. A respondent from an academic institution commented: "Workshops, school programs, and online awareness drives can educate users about how to identify cyber threats and what steps to take if they become a target of stalking." Respondents also noted that collaboration between the public and private sectors is vital. A participant from a regulatory body shared: "We have partnered with IT companies to conduct outreach programs that teach users how to safely navigate online spaces and protect their personal data."

Self-regulation and responsible online behaviour. Lastly, respondents stressed the importance of self-regulation in reducing the risks associated with cyberstalking. They emphasized that individuals should adopt responsible online behaviour, such as limiting the amount of personal information shared on public platforms. One respondent commented: "Users need to understand that what they post online often reaches a wider audience than they imagine. It's better to think twice before oversharing on social media." Another respondent also added: "Cyber safety starts with personal responsibility. Avoiding unnecessary exposure of private details is a key step in protecting oneself."

DISCUSSION

The study's findings indicate that victims' certain online behaviours contribute significantly to the risk of cyberstalking. In the Indian context, oversharing personal information on social media platforms, using unsecured devices, and engaging with unknown online individuals emerged as key behaviours that expose individuals to cyberstalking risks. This aligns with prior research that highlights how users' digital footprint can act as a gateway for perpetrators (Paat & Markham, 2020; AllahRakha, 2024). A similar pattern is observed in Malaysia, Singapore, and Indonesia, where increased digital connectivity has created new vulnerabilities. In Singapore, legal experts have emphasized that cyberstalking incidents often stem from social media misuse, leading to the Protection from Harassment Act (2014) being expanded to include digital forms of stalking (Rosli et al., 2021). In Malaysia, the enactment of Section 507A of the Penal Code (2023) acknowledges the role of digital surveillance and unwanted communication in cyberstalking, reflecting an awareness of how technological misuse contributes to victimization.

One respondent remarked, "Many victims unintentionally expose themselves by accepting friend requests from strangers or sharing too much personal updates online." This observation underscores the need for awareness campaigns, particularly in India (Rachna & Varshney, 2024) and Indonesia, where internet penetration is expanding and digital literacy remains inconsistent. Moreover, the respondents noted that the culture of constant connectivity and limited awareness of online safety amplify the risks. These findings resonate with theories such as Beck's risk-society framework, which identifies how technological advancements create new vulnerabilities in social life (Beck, 1992).

The study challenges the commonly held belief that cyberstalking is exclusively gender-motivated. While a majority of respondents acknowledged that women remain disproportionately affected, they also emphasized that men, too, are increasingly becoming victims of cyberstalking. One respondent stated: "It's not just women who face this… men also deal with cyberstalking."

This perspective may stem from the evolving gender dynamics in internet usage across Southeast Asia, where both men and women are active users of digital platforms. However, the findings also affirm existing literature, which highlights the systemic vulnerabilities women face due to patriarchal norms and gender-based violence (Sarkar & Rajan, 2023; Tarannum, 2024). Additionally, while the respondents acknowledged that anyone could perpetrate cyberstalking, they noted that male perpetrators continue to outnumber female ones. A similar observation was made in Malaysia and Singapore, where researchers noted that gender-neutral cyberstalking laws have increased awareness of male victimization. However, women remain the primary targets of digital harassment (Rosli et al., 2022).

Further, the findings reveal a mixed perception of the adequacy of legal protections against cyberstalking across jurisdictions. While respondents commended the inclusion of cyberstalking under Section 78 of the BNS Act in India, many expressed concerns about the implementation and enforcement of the law. A legal practitioner in India observed: "The law exists on paper, but victims often face delays in getting their cases registered, and the conviction rates remain low." This aligns with prior literature that reviews India's legal system's over-reliance on traditional methods to address cyberstalking (Rathnabai, 2023; Rachna & Varshney, 2024).

In Malaysia, the introduction of Section 507A of the Penal Code (2023) was seen as a crucial step, but enforcement remains a challenge, particularly in rural areas where digital crimes are underreported. Indonesia, which lacks a dedicated cyberstalking law, relies on the Electronic Information and Transactions (EIT) Law (2008), but respondents indicated that its broad language makes enforcement inconsistent. Singapore's Protection from Harassment Act (2014) was regarded as one of the strongest legal frameworks, with respondents emphasizing the effectiveness of protection orders and swift legal interventions.

The findings emphasize a multifaceted approach to mitigating cyberstalking risks, combining legal, technological, and educational strategies. Many respondents viewed reporting incidents to the police as a crucial step, though they acknowledged the reluctance of victims due to societal stigma and lack of confidence in law enforcement. One respondent remarked: "Filing a police report is essential, but victims often hesitate because they fear being blamed or not taken seriously." This highlights the importance of sensitizing law enforcement agencies to the psychological and social dimensions of cyberstalking.

Leveraging technology was another key modality suggested by respondents. They advocated for using security tools such as multi-factor authentication, blocking mechanisms, and cybersecurity software to protect against stalking. A respondent commented: "Technology is both the problem and the solution… victims need to know how to use it to safeguard themselves." Additionally, the role of awareness campaigns and digital education was highlighted as a preventive measure. Respondents called for collaborative efforts between the government, NGOs, and private entities to promote online safety. As one respondent put it: "We need a grassroots-level approach to teach internet users the basics of digital safety, especially in rural areas."

The findings also reflect a growing recognition of the victims' role in mitigating risks. However, placing excessive responsibility on victims without addressing systemic gaps risks perpetuating a culture of victim-blaming. While India and Indonesia still face structural challenges in law enforcement, Singapore's expedited protection orders and Malaysia's protective mechanisms under the Criminal Procedure Code (2024) serve as potential models for improving victim support across the region.

LESSONS FOR SOUTHEAST ASIA

India's experience highlights the need for stronger victim protection mechanisms, gender-sensitive training for law enforcement, and clearer legal definitions of cyberstalking. One of the key challenges identified in India is the gap between legal provisions and enforcement, which is similar to that observed in Indonesia. Indonesia, which lacks specific cyberstalking provisions, could benefit from adopting explicit legal frameworks similar to Malaysia's Section 507A of the Penal Code, which criminalizes stalking, including online harassment. The inclusion of protective orders under Malaysia's Criminal Procedure Code (2024) further enhances victim protection, a model that could be useful for jurisdictions like India and Indonesia, where victims often struggle to obtain preventive legal relief.

Another significant lesson comes from Singapore's Protection from Harassment Act (PHA), which provides expedited protection orders and civil remedies in addition to criminal penalties. The ability of victims in Singapore to obtain immediate legal relief within 24 hours contrasts with India's slow judicial processes, which often delay justice for cyberstalking victims. Implementing expedited protection orders in India and Indonesia would provide stronger legal safeguards against escalating online harassment.

A harmonized regional approach to cyberstalking legislation and enforcement is essential to effectively combat the problem. Countries in Southeast Asia could develop unified legal definitions and shared enforcement strategies to address the transnational nature of cybercrimes. Establishing cross-border cooperation mechanisms, particularly between law enforcement agencies, could facilitate faster investigation and prosecution of cyberstalking cases that involve perpetrators or victims in multiple jurisdictions.

Further, gender-sensitive training for law enforcement and judicial officers is a critical area for reform. India's experience highlights that victim-blaming attitudes among law enforcement officials hinder effective enforcement. Malaysia and Singapore have made significant progress in integrating digital literacy and victim-support programs into their legal systems. Expanding these initiatives regionally through joint training programs, information-sharing platforms, and awareness campaigns could improve law enforcement responses and enhance public understanding of cyberstalking laws.

Drawing on these comparative insights, this study advocates for a harmonized regional approach to addressing cyberstalking, emphasizing preventive legal measures, effective enforcement, and survivor-centered policies. Developing a regional framework or guidelines on cyberstalking laws in Southeast Asia could provide a cohesive legal foundation for addressing digital harassment, ensuring that victims receive adequate protection regardless of jurisdiction. Such measures would position Southeast Asia as a global leader in the fight against cyberstalking, setting new standards for legal innovation and victim-centered justice.

CONCLUSION

The findings of this study emphasize that cyberstalking is not merely a punishable offence but a pervasive and evolving threat that requires proactive intervention. Across jurisdictions, participants consistently highlighted that online behaviours, such as oversharing personal details on social media and unregulated internet usage, significantly increase vulnerability to cyberstalking. This emphasizes the urgent need for digital literacy initiatives and public awareness campaigns to promote safer online practices, particularly in India and Indonesia, where internet access is rapidly expanding. Contrary to common assumptions, the study revealed that cyberstalking is not exclusively a gendered crime, though women remain disproportionately affected. While cyberstalking laws in Malaysia and Singapore have adopted gender-neutral approaches, respondents emphasized that male perpetrators still outnumber female ones. The study also highlights significant disparities in legal protections across Southeast Asia. India, Malaysia, and Singapore have enacted statutory provisions criminalizing cyberstalking, while Indonesia lacks a dedicated cyberstalking law, relying instead on broader provisions within the Electronic Information and Transactions (EIT) Law (2008).

The adequacy of existing legal frameworks remains a contested issue. While some participants expressed concerns about the insufficiency of current laws, others argued that the issue lies in enforcement rather than legislation itself. Singapore's Protection from Harassment Act (2014) provides a strong model with expedited protection orders and civil remedies, which could serve as a reference for India and Indonesia. Similarly, Malaysia's recent amendments introducing protection orders under the Criminal Procedure Code (2024) offer valuable lessons for jurisdictions that lack victim-centered protections.

Importantly, non-legal interventions remain critical to addressing cyberstalking. Participants across jurisdictions emphasized technological tools for blocking and reporting stalkers, the role of digital platforms in moderating harmful content, and the necessity of collaborative public education campaigns. The study suggests that while individual responsibility for online safety is increasing, it must be complemented by systemic interventions to ensure that victims receive adequate protection. Stronger enforcement mechanisms, cross-jurisdictional legal cooperation, and enhanced victim support services are needed to create a safer digital environment in Southeast Asia. For policymakers, the implications are clear. A harmonized regional approach to cyberstalking legislation could bridge existing gaps and enhance victim protection across Malaysia, Singapore, Indonesia, and India. Collaboration between government agencies, technology platforms, and civil society is essential in developing survivor-centered legal frameworks and improving digital safety education.

ACKNOWLEDGEMENT

We sincerely thank all colleagues whose assistance and insights greatly supported this article.

REFERENCES

Abu-ulbeh, W., Altalhi, M., Abualigah, L. M., Almazroi, A. A., Sumari, P., & Gandomi, A. H. (2021). Cyberstalking victimization model using criminological theory: Systematic literature review, taxonomies, applications, tools, and validations. *Electronics*.

AllahRakha, N. (2024). Transformation of crimes (cybercrimes) in digital age. *International Journal of Law and Policy*, *2*(2). https://doi.org/10.59022/ijlp.156

Al-Rajhi, B. A. J. (2024). Evaluating UK legislation effectiveness in prosecuting cybercriminals and deterring cybercrimes: Identifying areas for improvement. *Pakistan Journal of Criminology, 16*(4), 701-721.

Asante, A., & Feng, X. (2021). Content-based technical solution for cyberstalking detection. In *Proceedings of the 2021 3rd International Conference on Computer Communication and the Internet (ICCCI)* (pp. 89-95). Nagoya, Japan. https://doi.org/10.1109/ICCCI51764.2021.9486770

Bailey, L., Hulley, J., Gomersall, T., Kirkman, G., Gibbs, G., & Jones, A. D. (2024). The networking of abuse: Intimate partner violence and the use of social technologies. *Criminal Justice and Behavior, 51*(2), 266-285. https://doi.org/10.1177/00938548231206827

Beck, U. (1992). *Risk society: Towards a new modernity*. Sage.

Boehnlein, T., Kretschmar, J., Regoeczi, W. et al. (2020). Responding to stalking victims: Perceptions, barriers, and directions for future research. *Journal of Family Violence, 35*, 755-768. https://doi.org/10.1007/s10896-020-00147-3

Brooks, N., Petherick, W., Kannan, A., Stapleton, P., & Davidson, S. (2021). Understanding female-perpetrated stalking. *Journal of Threat Assessment and Management, 8*(3), 65-76. https://doi.org/10.1037/tam0000162

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). Purposive sampling: Complex or simple? Research case examples. *Journal of Research in Nursing, 25*(8), 652-661. https://doi.org/10.1177/1744987120927206

Castells, M, & Pekka, H. (2002). *The information society and the welfare State: The Finnish Model.* Oxford.

Chan, H. C. O., & Sheridan, L. (2021). Who are the stalking victims? Exploring the victimization experiences and psychosocial characteristics of young male and female adults in Hong Kong. *Journal of Interpersonal Violence, 36*(21-22). https://doi.org/10.1177/0886260519889938

Chang, W. J. (2020). Cyberstalking and law enforcement. *Procedia Computer Science, 176*, 1188-1194. https://doi.org/10.1016/j.procs.2020.09.115

Deterding, N. M., & Waters, M. C. (2021). Flexible coding of in-depth interviews: A twenty-first-century approach. *Sociological Methods & Research, 50*(2), 708-739.

Dhir, A., Talwar, S., Budhiraja, S., & Islam, N. (2021). The dark side of social media: Stalking, online self-disclosure and problematic sleep. *International Journal of Consumer Studies*, 1373-1391.

Di Nicola, A. (2022). Towards digital organized crime and digital sociology of organized crime. *Trends Organized Crime*. https://doi.org/10.1007/s12117-022-09457-y

Fissel, E. R. (2022). Victims' perceptions of cyberstalking: An examination of perceived offender motivation. *American Journal of Criminal Justice, 47,* 161-175. https://doi.org/10.1007/s12103-021-09608-x

Fissel, E. R., Reyns, B. W., Nobles, M. R., Fisher, B. S., & Fox, K. A. (2024). Cyberstalking victims' experiences with fear versus other emotional responses to repeated online pursuit: Revisiting the fear standard among a national sample of young adults. *Crime & Delinquency, 70*(4), 1116-1147. https://doi.org/10.1177/00111287221096374

Geldenhuys, K. (2024). Technology-facilitated gender-based violence: A growing threat. *Servamus Community-based Safety and Security Magazine, 117*(10).

Giddens, A. (1990). *Consequences of modernity*.Polity Press.

Giddens, A. (1999). Risk and Responsibility. *Modern Law Review, 62*(1), 1-10.

Glazier, R. A., Boydstun, A. E., & Feezell, J. T. (2021). Self-coding: A method to assess semantic validity and bias when coding open-ended responses. *Research & Politics, 8*(3).

Hamin, Z., Kamaruddin, S., & Rosli, W. R. W. (2023). When the law is half-baked: A critique of the new anti-sexual harassment law in Malaysia. *Journal of Administrative Science, 20*(2), 256-267.

Harasgama, K. S., & Munasinghe, M. A. P. M. (2021). A comparative analysis of cyberstalking legislations in UK, Singapore, and Sri Lanka. *Sri Lanka Journal of Social Sciences and Humanities, 1*(2), 85-92.

Ho, H. T. N., & Luong, H. T. (2022). Research trends in cybercrime victimization during 2010-2020: A bibliometric analysis. *SN Social Sciences, 2*(4). https://doi.org/10.1007/s43545-021-00305-4

Humboldt, S. V., Ribeiro-Goncalves, J. A., & Leal, I. (2022). Bullying in old age: A qualitative study on older adults' perceptions about being bullied. *Journal of Interpersonal Violence, 37*(5-6), 2896-2919. https://doi.org/10.1177/0886260520943709

International Telecommunication Union. (2023, September 12*). Universal and meaningful connectivity by 2030.* Retrieved from https://www.itu.int/en/mediacentre/Pages/PR-2023-09-12-universal-and-meaningful-connectivity-by-2030.aspx

Kaur, M., & Saini, M. (2023). Indian government initiatives on cyberbullying: A case study on cyberbullying in Indian higher education institutions. *Education and Information Technologies, 28,* 581-615.

Kaur, P., Dhir, A., Tandon, A., Alzeiby, E. A., & Abohassan, A. A. (2021). A systematic literature review on cyberstalking: An analysis of past achievements and future promises. *Technological Forecasting and Social Change, 163*.

Khadim, S. W., Hassen, O. A., & Ibrahim, H. K. (2022). A review on the mechanism mitigating and eliminating internet crimes using modern technologies. *Wasit Journal of Computer and Mathematics Science, 1*(3), 50-68. https://doi.org/10.31185/wjcm.48

Khan, S., Nordin, R., & Hassan, M. S. (2023). A routine activity approach to understanding the reasons for technology-facilitated harassment against women in India. *IIUM Law Journal*, *31*(2), 229-252. https://doi.org/10.31436/iiumlj.v31i2.851

Kim, C., & Ferraresso, R. (2023). Examining technology-facilitated intimate partner violence: A systematic review of journal articles. *Trauma, Violence, & Abuse, 24*(3), 1325-1343. https://doi.org/10.1177/15248380211061402

Law Library of Congress. (2019). *Laws protecting journalists from online harassment: Australia, Brazil, Canada, England and Wales, Finland, France, Germany, Israel, Japan,*

Singapore, Spain, Turkey, international law. https://www.loc.gov/law/help/protecting-journalists/online-harassment.pdf

Martellozzo, E., Bleakley, P., Bradbury, P., Frost, S., & Short, E. (2023). Police responses to cyberstalking during the Covid-19 pandemic in the UK. *The Police Journal, 96*(4), 689-705. https://doi.org/10.1177/0032258X221113452

Ministry of Law Singapore. (2021). *Enhancements to the Protection from Harassment Act (POHA): Annex A*. https://www.mlaw.gov.sg/files/news/press-releases/2021/02/POHA-AnnexA.pdf

Paat, Y. F., & Markham, C. (2020). Digital crime, trauma, and abuse: Internet safety and cyber risks for adolescents and emerging adults in the 21st century. *Social Work in Mental Health, 19*(1), 18-40. https://doi.org/10.1080/15332985.2020.1845281

Parkhill, A. J., Nixon, M., & McEwan, T. E. (2022). A critical analysis of stalking theory and implications for research and practice. *Brhavioral Sciences & the Law, 40*(5), 562-583.

Permatasari, S. C., & Pujiyono, P. (2024). Criminal law policy as an attempt to overcome cyberstalking crimes in Indonesia. *International Journal of Social Science and Human Research, 7*(04), 2440–2443. https://doi.org/10.47191/ijsshr/v7-i04-56

Rachna & Varshney. R., (2024) Victims of cyberbullying and cyberstalking: An exploratory study of harassment perpetrated via the internet. *Library Progress International, 44*(3), 19213-19224.

Rao, S. (2022). Disturbing psycho-social trends in social media: The phenomena of cyber bullying and cyber stalking. *Global Media Journal, 20*(47), 1-6.

Rapisarda, S. S., & Kras, K. R. (2023). Cyberstalking. In D. Hummer & J. Byrne (Eds.), *Handbook on crime and technology* (pp. 303-333). Edward Elgar Publishing.

Rathnabai, S. A. (2023). Nurturing mental and emotional well-being in the cyberspace. *Indian Journal of Health and Wellbeing, 14*(4), 538-542.

Rosli, W. R. W., Hamin, Z., Rani, A. R. A., Kamaruddin, S., & Hassan, R. A. (2021). Non-criminalisation of cyberstalking and its impact on justice for victims: Some evidence from Malaysia. *International Journal of Academic Research in Business and Social Sciences, 11*(6), 1257-1266.

Rosli, W. R. W., Kamaruddin, S., Rani, A. R. A., Saufi, N. N. M., & Husain, N. M. (2022). Mystalk Alert: A Response to Cyberstalking in Malaysia. *Telematique*, *21*(1), 5800-5809.

Sari, A. P., & Suryani, N. (2023). The role of digital literacy in preventing cyberstalking among adolescents in Indonesia. *International Review of Humanities Studies, 8*(1), 45-60.

Sarkar, S., & Rajan, B. (2023). Materiality and discursivity of cyber violence against women in India. *Journal of Creative Communications, 18*(1), 109-123. https://doi.org/10.1177/0973258621992273

Shanmugasundaram, M. & Tamilarasu, A. (2023). The impact of digital technology, social Media, and artificial intelligence on cognitive functions: A review. *Frontiers Cognition, 2.*

Stevens, F., Nurse, J. R. C., & Arief, B. (2021). Cyber stalking, cyber harassment, and adult mental health: A systematic review, *Cyberpsychology, Behavior, and Social Networking, 24*(6). https://doi.org/10.1089/cyber.2020.0253

Storey, J. E., Pina, A., & Williams, C. S. (2023). The impact of stalking and its predictors: Characterizing the needs of stalking victims. *Journal of Interpersonal Violence*, *38*(21-22), 11569-11594. https://doi.org/10.1177/08862605231185303

Tarannum, M. (2024). Cyber crimes against women in India: An analysis. *Central University of Kashmir Law Review*, *4*, 133-147.

Todd, C., Bryce, J., & Franqueira, V. N. L. (2020). Technology, cyberstalking and domestic homicide: Informing prevention and response strategies. *Policing and Society*, *31*(1), 82-99. https://doi.org/10.1080/10439463.2020.1758698

Women's Aid Organisation. (2023, May 31). Malaysia's anti-stalking law now operational. *Women's Aid Organisation.* https://wao.org.my/malaysias-anti-stalking-law-now-operational/

Yong, L. (2024, October 16). *Protection from Harassment Act (POHA): A guide to harassment law and protection orders in Singapore.* Guardian Law. https://guardianlaw.com.sg/posts/protection-from-harassment-act-poha-a-guide-to-harassment-law-and-protection-orders-in-singapore/

BIODATA OF AUTHORS:

Samina Khan (Corresponding author)
Faculty of Law,
Universiti Kebangsaan Malaysia, Malaysia
Email: amu.samina@gmail.com

Rohaida Nordin
Faculty of Law,
Universiti Kebangsaan Malaysia, Malaysia
Email: rohaidanordin@ukm.edu.my

Muhamad Sayuti Hassan
Faculty of Law,
Universiti Kebangsaan Malaysia, Malaysia
Email: sayutihassan@ukm.edu.my