Asian journal of International Peace and Security (AJIPS)

ISSN-e: 2707-8809

Vol. 7, No. 2, (2023, Summer), 41-56

Cyber Stalking: Victims Vs Legal Protections

Zainab Bibi,[1] & Ambreen Abbasi[2]

Abstract:

The concept of cyber stalking is not new to cybercrime category but many countries are still promulgating laws to protect cyber space from this intimidating behavior; however, some countries has taken it a crime against female only and some has been very late to regulate cyberspace. Therefore, with the legislative comparison between India and the United Kingdom (UK), the clear stance on cyber stalking will be presented as UK legal system is yet to promulgate cyber stalking regulations while India has only considered female in the role of victim rather than mentioning anyone subject to cyber stalking. On the other hand, the legal perspective on cyber stalking of the developed countries such as Japan, Poland, and Singapore would help to analyze the problem in detail. The legislative provisions elucidate the comprehension regarding efforts that have been put in place by the international community to prevent cyber stalking and to protect their citizen. Thus, the present research is conducted by comparison of legal provisions of recently promulgating laws regarding cyber stalking in different states and for this purpose comparative study methodology is adopted.

Keywords: India, UK, Japan, cyber stalking, international perspective, victim, legal protection

INTRODUCTION

The idea of a world without technology is almost impossible. Technology is used for many things, including employment, shopping, recreation, and other things. On one hand, technology saves time and provides everything one needs, but on the negative side it has given rise to a brand-new category of crime known as cybercrime (Sakshi et. al, 2022). Any crime committed using a computer as a target, tool, or other method is referred to cybercrime. The majority of cybercrime focuses on the data of a person, business, organization, community, or government (Shambhavee, 2019).

Cyberstalking is one of them; therefore, a continuous sequence of persistently unwelcome actions carried out through digital communication technologies is known as cyber stalking (Thelwall, 2002). Cyberstalking is when a person repeatedly tries to get in touch with another person with the aim of affecting their life or frightening them (Sadotra, 2015). The development of information technology has also made it possible for stalkers to conceal their identity, allowing them to commit

[1] Holds LLM (Human Rights Law) degree from Faculty of Shariah & Law, International Islamic University, Islamabad, Pakistan. Email: zainabbibi2468@gmail.com

[2] Assistant Professor, Faculty of Shariah & Law, International Islamic University Islamabad. Email: ambreen.abbasi@iiu.edu.pk

crimes comfortably while being unknown (Drebing et. al. 2014). One of the main benefits of a cyber-stalker is that they don't have to leave their house to find their targets; in other words, they do not fear physical harm because they think they are untouchable in cyberspace (Thapa & Kumar, 2011). Internet, email, electronic communications, and social networking sites like Facebook, Instagram, etc. are the main channels by which cyberstalking occurs and the severity of cyber stalking has gotten worse with time (Citron. 2014).

The rate of cybercrime keeps on rising daily as a result of rapid growth of technology with the passage of time. Cyberstalking is one such cyberattack that needs prompt action (Jaishankar, 2005). Most of the time, women who are stalked and harassed by men or young children and being pursued by adult predators are the victims (Willard, 2006). Cyberstalking is the act of following and pursuing someone online, violating their privacy by keeping tabs on every move they make (Thelwall, 2002). It can also be seen as a sort of harassment that upends the victim's life and makes them feel extremely scared and afraid (Schwarzer, 2000).

Furthermore, the comparative study of international legal perspective with reference to cyber stalking (Halder & Jaishankar, 2011) highlights information regarding legal framework and its practices in United Kingdom (UK) and India to deal with the said crime. Along-with the briefing of the system and protection provided by the developed countries like Japan, Poland and Singapore, it would be essential to analyze legal viewpoint of cyber stalking.

INTERNATIONAL PERSPECTIVE OF CYBER STALKING

English author John Austin, a prominent authority on law, says "International law is not a true law," but a set of morally bound guidelines. According to him, international law is not a law because it has no originating source and no supporting sanctions. Austin defined international law as a positive code of conduct that reflects the attitudes or beliefs of most states (Austin, n.d.).

As skilled stalkers are adept at hiding behind false personas, it is challenging to locate and repel them (Citron, 2009). Therefore, a fine or perhaps detention may be imposed, depending on how serious the situation is (Shimizu, 2013). However, international law is not enforceable and the problem of cybercrime cannot be resolved solely through international law (Drebing et. al. 2014). Hence, each state must enact its own legislations governing freedoms and violations in the area of cyber stalking (Sadotra, 2015).

While free and organized media also play a key role in educating people and giving them the ability to express their opinions, while the right to information (RTI) is a crucial component of holding an evaluation (Citron, 2014). All things considered, it is essential to have a system that gives individuals the ability to develop and protect their right to knowledge, control and limit covert public authority actions, and ensure freedom and diversity of media (Alam, 2015).

Legal Analysis of Social Media Laws in UK, and India

In the UK, the law on communication was established in 1988, but due to the advanced technological era, the need for social media laws or regulations is felt in the country (Whitehead, 2011). If the discussion is about protecting women or children, the issue of restricting the freedom of information is not significant as long as it serves the interests of the state or children in particular (Condry, 2010). If the law is unanimous and outlines the entire scope of regulatory and

policing authorities, the female victim of cyber stalking can protect herself from online harassment (Bocij, 2004). Information freedom is violated to the extent that cyber stalking uses information while breaching the right to privacy (Citron, 2014).

Increased cybercrime has been seen in India as a result of the quick adoption and expansion of internet-connected gadgets, as well as the facilitation of communications technologies (Jaishankar, 2008). These technologies give stalkers the ability to target victims remotely while also offering anonymity and convenience (Vitak, 2017). Everywhere individuals use information and communication technologies and cyberstalking is increasingly common with women being the most frequently targeted demographic (Duggal, 2009). As per reports, majority of the victims of Cyber stalking are considered to be females; however, in reality, stalking has the potential to victimize anyone, whether man or a woman.

Cyber Stalking in UK's Law

In the UK even though cyber gender harassment cases are skillfully handled by current anti-harassment regulations, but secondary victimization by police and criminal justice systems still happens in the UK (Condry, 2010). Both the issue of recognizing crimes against women committed online and taking meaningful action to stop such crimes hang over these issues (Halder & Jaishankar, 2011).

It is a harsh reality that unlike other crimes that are officially recognized as offenses, cyberstalking cases do not actually provide the police the authority to search and take anything (Whitehead, 2011). The report also made note of the fact that many victims complain about the police's subpar reaction to reports of such offenses (Whitehead, 2011). It is reasonable to assume that female victims of cyber-gender harassment, which can encompass stalking (Ellison & Akdeniz, 1998), would receive harsh treatment due to the lower level of stigma attached to such actions. Sending Communications is just one of the many crimes that may now be committed on social media. It may be possible to control Cyber Stalking to some extent using laws like the Malicious Communications Act (MCA) of 1988 (particularly, section 1) and the Communications Act of 2003 that may be used to prosecute a violation (Sadotra, 2015).

Malicious Communications Act (MCA) of 1988

Sending letters with the intention of causing stress or unhappiness is a violation of Section 1.

> Section 1: Offence of sending letters etc. with intent to cause distress or anxiety.
>
> (1) Any person who sends to another person—
>
> (a) A letter, an electronic communication or article of any description which conveys—
>
> (i) A message which is indecent or grossly offensive;
>
> (ii) A threat; or
>
> (iii) Information which is false and known or believed to be false by the sender;

MCA 1988 elaborates as any person who sends a letter, an email, or an article of any kind that contains an offensive or terrifyingly threatening message, a threat or piece of information that is false and the sender knows or admits it is false, or any electronic communication that is entirely or partially of a sickening or terrifyingly unfriendly nature is guilty of an offense if his intentions are those already mentioned, or one of them. If found guilty of either the offense already addressed, the

offender faces a maximum two-year detention sentence as well as a one-year sentence in prison or a fine or both (c.37).

The Communication Act, 2003

Section 127 of the Communication Act 2003 focuses on improper use of open social media platforms. It states that a person may be charged with a crime if they use an electronic network or another method to send someone a message that is extremely hostile, revolting, vulgar, threatening, or causes another person distress even though they are aware the message is false and they continue to use the network for communication. As a result, anyone found guilty of this will be sentenced to a quarterly period in prison, a fine, or both (c. 21).

Online Harms Regulations

Because cyber stalking happens frequently on social media, the UK has established social media regulations to lessen its effects and causes while maintaining the possibility that it will be charged as a crime (Dooley, 2009). In April 2019, a white paper on internet dangers was released. This clarified the government's stance on "content or activity that harms individual users, particularly children, or threatens way of life in the UK" (Woodhouse, n.d.).

The new oversight framework would not require partnerships to completely remove specific legal content in order to guarantee information freedom. In order to reliably and transparently approve this, the rules explicitly describe what behavior and content would be considered acceptable on their respective localities (Shambhavee, 2019). It would be necessary to "expeditiously" remove any illegal content. In relation to terrorist content and child exploitation and abuse, strong measures would be necessary (Woodhouse, n.d.).

If social media businesses fail to stop online abuses such racial hate crimes, they might be fined up to 10percent of their annual revenue or 18 million pounds ($25 million), and senior managers could be prosecuted (Holden, 2021). Additionally, this Online Safety Bill strives to improve the freedom of expression, ensures democratic political discourse, and provides for the protection of journalistic content (Franks, 2010). “Tech corporations must be held accountable and must safeguard the safety of the British people. Penalties would be applied if they don't,” Interior Minister Priti Patel said (Holden, 2021).

It must be understood, in the opinion of the researcher, that social media regulation is still urgently needed by examining the UK's ongoing regulations. For many years, the UK has worked to control social media (Vitak, 2017). The only things that can be managed and regulated by rules are information freedom and cyber stalking (Shimizu, 2013). If criticizing the protection of cyberspace just seeks to exploit the freedom of information as a tool to halt the regulatory processes, then it should not be acknowledged (Ellison & Akdeniz, 1998).

According to James Rhodes v. OPO (by his case partner BHM), decided by the Supreme Court of the UK, it is impossible to imagine any circumstances in which conduct is not deceptive, intimidating, or on the other hand, potentially destructive, affording the opportunity to engage in wrongdoing for the intentional violation of another person's right to individual security (Willard, 2006). Truth reporting is legitimate and this should not be interpreted to mean that the right to disclosure is

absolute, as there may be a duty to treat information as private or confidential on the part of the individual (James Rhodes v. OPO , 2015).

Cyber Stalking in India's Laws

The section focuses on the administrative provisions that are mentioned in the Indian legislation with regard to the Information Technology Act (ITA) of 2000 and the Indian Penal Code (IPC) of 1860 even more explicitly. It explains how these laws apply to cyber stalking and under what circumstances the offender may be held accountable (Shah, 2014). India's laws are biased because government officials saw women as the population group that was most at risk. Thus, every provision revolves around protecting women; nevertheless, from another angle, it may be argued that lawmakers may have thought women to be more susceptible in society than men. (Keswani, 2017)

There are no immediate measures in place to address the problem of cyber stalking. Nevertheless, the study made an effort to explain the few sections of the IPC and the ITA 2000 that has any connection to this crime, and it provided an explanation of how these provisions relate to the offense (Sadotra, 2015).

Indian Penal Code 1860

First Section 354D of IPC 1860 characterizes "stalking." It peruses as follows:

> (1) Any man who—i. follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or monitors the use by a woman of the internet, email or any other form of electronic communication commits the offence of stalking (The Criminal Law (Amendment) Act, 2013).

Following the Delhi attack case, the clause was added by the Criminal Amendment Act of 2013 (Duggal, 2009). It considers both traditional stalking and online stalking. The statute depicts its application to actions that constitute the crime of stalking. The clause clearly states that anyone who seeks to monitor a woman's online activities is engaged in stalking (Jaishankar, 2008). As a result, the stalker violates Section 354D of the IPC if he commits any of the acts listed in the part (The Criminal Law (Amendment) Act , 2013).

This section contains many caveats, for instance, it only considers "females" to be the person in issue and ignores the possibility that even men could be the person being referred to (Thapa & Kumar, 2011). The Section makes it clear that anyone attempting to monitor a female's online behavior through email or another form of electronic contact runs the possibility of being charged with the crime of cyber stalking (Aravinth, 2019). It is clear that women are the main focus. It is one-sided enactment in this sense. Additionally, the lawmakers have not mentioned the "strategy for monitoring." (The Criminal Law (Amendment) Act , 2013).

The IPC has limitations pertaining to cyberstalking in Section 354D. There was no specific law pertaining to cyber stalking prior to the Criminal Amendment Act of 2013, but the Amendment Act has introduced the legal provisions of this offense (Chahal, 2019). This section can be used to punish a male who stalks a woman or makes an effort to get in touch with her in any way, whether in person or online (Aravinth, 2019). For the first time offense of stalking, a person can receive up

to 3 years in prison and a fine, and for the second time offense, they can receive up to 5 years in prison and a fine (The Criminal Law (Amendment) Act , 2013).

Second, the IPC's Section 292 defines "obscenity." the act of sending vulgar content to the victim via email, text message, social networking site, etc. and is considered cyber stalking (Hess, 2014). When a stalker tries to defame another person by posting vulgar content online thinking that the target would read, see, or hear the content of the material, he will be held accountable for the offense under Section 292 of the IPC 1860.

Third, the IPC's Section 507 addresses "criminal upsetting by mysterious communication." This paragraph conveys that it is a crime when a stalker makes an effort to hide his identity from the victim so that she remains unaware of the source of the torture. As a result, it ensures the unidentified character trait of a cyber-stalker (Aravinth, 2019). When a stalker makes an effort to conceal their identity, they violation this provision of IPC 1860.

Fourth, Section 509 of IPC relates to quietness of women examined as follows;

> Word, motion or act proposed to disrespect the modesty of a lady. Whoever, expecting to affront the unobtrusiveness of any lady, expresses any word, makes any solid or signal, or shows any item, aiming that such word or sound will be heard, or that such motion or article will be seen, by such lady, or interferes with the protection of such lady, will be punished.

Under section 509 of the IPC, a stalker can be held accountable if their actions endanger the woman's safety through physical contact, verbal messages, or material shared online (Jaishankar, 2011). Numerous deficiencies exist in Section 509. Some of them include: it is an unequal strategy since it concentrates on a woman's modesty and neglects the fact that this negative behavior of cyber stalking is universal in nature and that even men might be the target of such violation (Chahal, 2019). According to the IPC 1860, the words, sound, or symbol must be said, heard, and seen individually for this need to be met. Since words cannot be spoken, motion cannot be seen, and sound cannot be heard online, cyber stalkers can surely escape punishment under this clause (Zarina, 2016).

INFORMATION TECHNOLOGY ACT, 2000

First of all, Section 292 of the IPC and Section 67 of the ITA 2000 are exactly the same. In addition, sections 67B and 66E of the IT Act 2000 cover this offense. The stalker will be guilty of an offense under Section 67 of the ITA 2000 if he attempts to publish any lewd content about the victim using online media that is in an electronic structure. It conveys that a stalker who sends or uploads any lewd material to the victim via electronic media will be guilty and subject to a five-year prison sentence and a fine of Rs. 1 lakh under Section 67 of the Act.

The concept of a cyberstalking offense is covered by Section 67A of the ITA 2000 and "Material containing sexually explicit activity" is a brand-new category created by Section 67A of ITA 2000 and constitute offence if they attempt to distribute any "sexually explicit" content through messages, emails, or other online media.

The ITA 2000's Section 67B, which was added too late by the Amendment Act of 2008 emphasized the threat stalkers pose to children under the age of 18 by disseminating materials showing young people engaging in sexual activity.

Furthermore, "voyeurism" is governed by Section 66E of the ITA 2000 and Section 354C of the IPC. According to Section 66E, there will be consequences for anyone who "deliberately or intentionally captures, distributes or sends the picture of a private zone of any individual without that person's consent under circumstances that violate that person's privacy."

Both the ITA 2000 and the IPC of 1860 ambiguously lack provisions for dealing with the problem of cyber stalking and the insulting or compromising messages sent by the stalker while following the victim through messages, calls, communication, or by disseminating web journals under the name of the person being referred to (Sakshi et. al, 2022). Although there is no express method that solely deals with this offense, it is possible to penalize the offender in accordance with the requirements of the recently referenced Acts as mentioned in the above section (Aravinth, 2019). Although the negative behavior's execution is simple, its effects last a long time (Mantilla, 2015). It may have a negative impact on the victim's physical and mental health (Ferdon, 2007). The punishment provided under current laws needs to be increased while keeping the victim's safety in mind (Gokani, n.d.).

Contrary to other nations, India has a much lower number of complaints reported than would be expected given the high frequency (Chahal, 2019). We concentrated on the situations of two women in an effort to capture cyberstalking experiences in India as well as the context and factors that compel the women and their families to make choices to cope with it.

Cases of the Cyber Space

1. The Vinu Priya Case is a very recent and well-publicised case. The victim in the current situation was a 21-year-old BSc. graduate. When the first photo appeared on June 23, she told her father, who then lodged a complaint with the Cyber Crime Cell. Vinupriya's father was informed by the police that they would find the culprit in about 14 days, but they either lacked the investigative skills or were simply uninterested in finding out who modified the photo or both. A member of the Cyber Crime Cell allegedly asked the father for a cell phone to finish the inspection. According to Vinupriya's father, he gave the policeman a cell phone for Rs 2,000 and even after they accepted bribes, they didnot get justice. Vinupriya suffered harm after a second vulgar photo was released on Facebook on June 26. The investigating officials had lately assumed that she had sent those pictures to someone, and that it was likely an unwelcome ex, but now they were being uploaded. These were the lines used to address Vinupriya. On June 27, she committed suicide (Palanisamy Petitioner v. State of Tamil Nadu).
2. Sharmistha Mukherjee, the daughter of President Pranab Mukharjee, was allegedly stalked by a man who allegedly tapped her Facebook account and sent expressly clear-cut messages. She filed a complaint with the Delhi Police's Cyber Crime division. According to the police, the complainant received the "lewd" texts via Facebook Messenger. According to his online profile, the sender is a renter of Nauhati in Hooghly, West Bengal. Mukherjee uploaded screenshots of the messages that appeared and stated that she decided to go against online provocation because not doing so would just strengthen him. She said;

This spoil Partha Mandal is directing me explicit messages. My 1st reaction was to ignore and block him. But then I thought the silence would encourage him to find other victims. Just blocking and reporting is not enough. I strongly feel such people should be publicly exposed and humiliated. I'm posting screenshots of his profile and messages he sent me. I'm also tagging him. Please share this post and tag this rat as a message that these pervert acts will not be taken lightly, she wrote.

Since there is no special stalking law, we ?? ourselves experienced significant difficulties in avoiding becoming victims. By using the example of police complaints in India, it can be seen that because of bribery, police conditions are not up to par. As a result, laymen who are the victims of such crimes suffer greatly (Sharma, 2021).

Information Technology (Intermediary Guidelines & Digital Media Ethics Code) Rules, 2021

The Ministry of Electronics and Information Technology and the Ministry of Information and Broadcasting (MIB), Government of India, have notified new rules under Section 87 of the ITA 2000 for monitoring social media digital media platforms on February 25, 2021, after years of discussions and debates. The Information Technology (Intermediaries Guidelines) Rules 2011 are replaced by the Intermediary Rules 2021, which aim to create a unified, gentle supervision system for social media platforms, digital media, over the top (OTT) platforms, etc. (Dhubey *et. al.* 2021).

When considering the scope and type of the proposed framework for regulating social media and digital media platforms in India, the government of India has made an effort to take note of the models already in place in other nations, including Singapore, Australia, the European Union, and the United Kingdom (Sharma, 2021). The Intermediary Guidelines were created in an effort to create a three-tiered grievance redressal system and a classic soft-touch, self-regulatory architecture for digital media platforms operating in India (The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, n.d.).

However, the social media and digital media platforms may find it challenging to comply with the Intermediary Guidelines, which are also perceived as an effort to limit freedom of information to stifle free speech and expression (Sakshi et. al., 2022). The protection and defense of the rights of social media victims against the right to personal expression while limiting the freedom of information would require negotiating a fine line (Machanda & Kumar, 2021).

In some instances, such as when they regulate significant social media intermediaries and online publishers and demand that certain intermediaries identify the first source of information, the Rules, in the opinion of the researcher, may go beyond the authority granted by the Act (Chahal, 2019). When law enforcement organizations question intermediaries for information, there are no procedural safeguards in place. These regulations must address information freedom and explicitly address cyber stalking and the steps taken to prevent it (Powell, 2016).

PRACTICES OF DEVELOPED COUNTRIES ON CYBER STALKING

It is important to raise public awareness of the relatively recent criminalization of stalking. Between the sixteenth and twentieth centuries, the English word "stalk" was used to describe the act of creeping up to catch or hurt a person or animal (Megarry, 2014). However, the definition of this phrase has changed recently. In the latter half of the twentieth century, the term "stalking" was

first used in the media to describe the behavior of someone who continuously pursues others and annoys or frightens them (Hess, 2014). As society has grown more conscious of the fact that continually pursuing, frightening, or hurting others constitutes criminal or illegal behavior, stalking and stalker are now phrases used to describe such criminal activity and offenders (Spitzberg).

Japan

Even now, most people find Japan to be a narrow-minded nation when it comes to discussing private things. This is one of the reasons that not all incidents of stalking or violent behavior at home or online are reported (Megarry, 2014). While it may seem absurd and ridiculous to the majority of Westerners in this day and age, the humiliation of "causing others trouble" and "shame" is still seen as the standard in Japan (Japan: Anti-Stalking Act, n.d.). Due to advancement in technology, stalking instances have recently increased, but it is difficult to estimate their exact numbers because of cyber stalking and victims' reluctance to come forward (Tedx, 2015).

The most recent statistics about the response to stalker and domestic violence crimes are released by the National Police Agency at the beginning of March 2020. The gender distribution is readily obvious and hardly surprising (“Number of consultations,” 2023). In general, 84percent of victims and more than 80percent of offenders are men. The majority of stalkers are in their twenties or thirties with highest ratio fall in twenties (Tedx, 2015).

The police themselves suggested that both victims and stalkers receive assistance, or assistance provided or mediated by professionals, including teaching harm deterrence techniques, negotiation strategies, introduction to private organizations that carry out damage prevention activities, use of police facilities as a place to discuss damage prevention, teaching or lending items that contribute to damage prevention, delivery of documents indicating that cautions have been carried out, and so on (Nikolova, 2020).

Japan is toughening up its laws against internet abuse and cyberbullying. A plan to modify the penal code was approved by the Japanese, making online "insults" subject to a maximum fine of $2,500 and a one-year prison sentence (Siripala, 2022). However, fear hovers that the constitution's protection of free speech may be jeopardized by the blurry line between an insult and criticism (Kyodo, 2017)

The modifications were brought about by the suicide of a 22-year-old reality television and professional wrestler Kimura Hana in 2020, who did so after being bombarded with abusive insults on social media (Siripala, 2022). After the two perpetrators of the social media abuse received a mere warning, Kimura's mother Kyoko began a campaign to toughen the laws against cyberbullying.

Under the existing laws, they could have received a light prison sentence of less than 30 days and a fine of no more than 10,000 yen (roughly $73). Kimura Kyoko supported the change, contending that the penal code was not strict enough to deter recurrent offenders. Most criminal complaints being made have often resulted in 9,000 yen ($65) fines. The penal code's classifications and punishments have not been changed in 115 years (Kyodo, 2017). According to the Ministry of Justice, educational programs would be tailored to each individual's needs that too include a "rehabilitation" component rather than a punishment (Siripala, 2022).

Poland

The word "cyber stalking" in Polish Law comes from the combination of the words "cyber" and "threat," both imply computers, the web, or other electronic devices, as well as "mercilessness" (Sowalski, 2010). That particular feeling of fear was popular at the turn of the twentieth and beginning of the twenty first century. The Polish penal code's Article 190a addresses cyber stalking and provides appropriate penalties and remedies (Pietkiewicz & Trender, 2018). Stalking is currently illegal in Poland under a single legal standard that does not differentiate between traditional stalking and cyberstalking (Ellison & Akdeniz, 1998). According to Article 190a S1 (c.c), anyone who, by the persistent harassment of another person or another person's next of kin, causes a legitimate sense of danger or seriously violates the person's privacy is punishable to imprisonment for up to three years (Pietkiewicz & Trender, 2018).

Stalking is punishable under Article 190a of the Criminal Code, which was added to the law in 2011 (Hypś et. al. 2012). The necessity to develop a safeguard (Ferdon, 2007) for those who have been subjected to unfavorable social interactions, such as stalking, drove this decision (Pietkiewicz & Trender, 2018). According to 2009 surveys conducted by the Polish Ministry of Justice to ascertain the scope of this sort of activity nationwide, 9.9%percentof respondents said they had experienced stalking, and unsolicited emails were one of the main forms of persistent harassment (Pietkiewicz & Trender, 2018).

Prior to the 6th June 2011 amendment (the Penal Code Journal of Laws on 2001 No 72 pos. 381), the law enforcement authorities' ability to combat stalking was severely constrained by the laws in place because they did not fully protect victims (Hypś et. al. 2012). Only when the perpetrator's activities came within the following list of prohibited crimes—punishable threats (Art. 190 c.c.)—was effective action conceivable (Zygmunt Ł. (2013) w: Trybus M., 2013).

The most significant statutory provisions of the June 6th amendment describe stalking as a multifaceted offense in which harassment entails persecuting the victim through repeated acts that distress, torture, bully, or upset them (Śledziewski, 2013). The behavior that is punishable may include actions that are evaluated as one legal action (Hypś et. al. 2012).

According to the 2011 addition of Art. 190a to the Polish Penal Code, anyone who persistently harasses a person and causes them feel threatened or seriously invades their privacy will face a sentence of up to 3 years in prison (Pietkiewicz & Trender, 2018). A new regulation (Article 190a of the Penal code) addresses the use of personal information or images for malicious purposes as well (Hypś, et. al. 2012).

Singapore

Stalking is a behavior towards a person that results in severe or profound suffering. This adds to frequent unwanted contacts without cause, the dissemination of information to third parties via email or letter, upsetting workplace interactions, physical and online stalking, phone messages, insults, threats, contacting, and rude language (Treder, & Opalska, 2016). The Protection from Harassment Act (POHA), which went into effect in November 2014, seeks to protect individuals from becoming the targets of harassment or stalking, whether they do suffer it online or offline. Most recently, a series of adjustments were made to protect those who had been deceived to

improve assurance and increase the sufficiency of the POHA's lawbreaker and common measures against demonstrations of provocation ("Guide to Singapore's Protection," 2022).

For instance, in PP v. Lai Zhi Heng, the accused was charged with stalking after he repeatedly followed the victim, sent her multiple SMS, and even posted flyers with undressed pictures of her in public places close to her house (Treder M. w: Opalska A., 2016). The victim endured "anguish and torment" as a result of this conduct for about two years. Victim can file a Magistrate's Complaint or report being stalked to the police. In addition to filing a police report or a magistrate's complaint for the unlawful stalking, you have the option of suing the stalker for monetary damages ("Guide to Singapore's Protection," 2022).

Protection Order

To prevent further stalking, a victim may also file a protection order (hereafter "PO") against the stalker. According to the POHA, disobeying a protective order is illegal. A PO suggested ways to prevent harassment, including: forbidding the perpetrator from harassing the victim in any way; requiring that no one spread harassing communications or continue to announce such conversations; referring the perpetrator and/or victim to mediation or psychotherapy; and/or offering any other guidance necessary to ensure that a PO is effective.

Study comes to a close with some observations made by EU President Ursula von der Leyen at a special talk she delivered on January 26, 2021, to the Davos agenda week. According to her, social media cannot be used to undermine democracy (Leyen, 2021). She said

> What is illegal offline should be illegal online too, and we want the platforms to be transparent about how their algorithms work because we cannot accept a decision that has a far-reaching impact on our democracy, taken by computer programs alone. We want it clearly lay down that internet companies take responsibility for the manner in which they disseminate, promote and remove content (Leyen, 2021).

A new regulation being proposed by the EU would oblige tech companies to share data with competitors and authorities, explain their algorithms, remove unlawful information, and are upfront about their advertising (Lomba, 2020). Additionally, Leyen stated that for the values we admire in the offline world to be respected online, we need to restrain the huge power of the major cyber firms (Leyen, 2021).

Comparison among Cyber Stalking Laws

By presenting a detail of actual practices, this study offers a quick examination of developed countries' cyber stalking regulations. A comparative legal framework is now presented, one that offers cyber stalkers penalties and punishments in addition to protection and assistance for victims (see table no 1). It consists upon comparisons of legal system between Japan Poland, Singapore, India and UK. The table no.1 discusses Legal Framework, and relating provisions, Years of Promulgation of Laws and Punishments (detainment or fine or both), assistance of victim and the institutions that are responsible for the dispensation of justice.

Table 1.

Comparison summary of Japan, Poland and Singapore's Cyber Stalking Laws:

S. No	Category	Japan	Poland	Singapore	India	UK
1.	**Legal Framework**	Act no. 21	Polish Penal code	POHA	1. Indian Penal Code (IPC) 2. Information Technology Act (ITA)	1. Malicious Communication Act (MCA) 2.Communication Act (CA)
2.	**Provision**	Art. 1	Art. 190a amended S1, S2, S3	Sec. 3 & 7	IPC Sections: 354D, 292, 507, 509 ITA Sections: 62, 67A, 67B, 66E	Sec 1 MCA Sec 127 CA
3.	**Year**	2000	2011	2014	IPC 1860 ITA 2000	MCA 1988 CA 2003
4.	**Detainment + Fine**	Yes	3 Years to 10 Years	6 Months and fine upto $5000	3 Years and Fine (ITA 2000)	MCA: 2 years or fine (or both) CA: 6 Months or fine
5.	**Assistance to victims**	Police by the standards of National Public Safety commission	Protection Order under Criminal Code, Article 41aS1	Protection Order under POHA	Police Cyber Cell	Illicit content to be eliminated expeditiously
6.	**Role in assistance (authority to provide help)**	Police	Court	Court	Court	Court

CONCLUSION

Cyberstalking is an exacerbating issue and is being seriously regulated by the state legislative authorities. The international community is contemplating the promulgation of codified provisions and protections against cyberstalking. Moreover, comparative analysis of the cyber stalking laws of certain countries has clarified each state's serious efforts to control cyber stalking, especially to protect cyberspace from cyber malpractices. Even though states are making efforts ranging from the promulgation of laws to providing rehabilitation services, we must be vigilant about our actions being carried out in cyberspace.

Each state is making every effort to create new legislation that will aid in preventing and stopping harassment, stalking, and other crimes, both online and off; however, one must be cautious, though, and refrain from disclosing too much personal information and data on public forums like social media. As is often said, prevention is better than cure. Regardless of whether you have been the victim of stalking or not, your online and offline behaviors play a crucial role in safety.

Avoid leaving too many traces of yourself behind, especially online, by posting details about your residence or current location as these could give stalkers ideas about when and where to attack. If you are already a victim of stalking, you should cease disclosing too much personal information because it may open you up to further trouble. If you are being stalked in person and you are aware

of it, delete the offender from your online media accounts and avoid collaborating or communicating with him.

As far as legislative protection is concerned, serious legislative steps are under several states' consideration and are already in the drafting process. While some countries have already clearly granted protection against cyberstalking, we must also be very careful about secrecy and privacy policies. On the contrary, policymakers also make sure to frame precise and brief terms and conditions to facilitate readers' understanding and their agreement to the privacy policy.

References:

Alam, M. A. (2015, Aug.). *Freedom of information and media laws in Pakistan*. Centre for Peace and Development Initiatives. http://www.cpdi-pakistan.org/wp- content/uploads/2015/08/Right-to-Information-and-Media-Laws-in-Pakistan1.pdf

Aravinth, B. (2019). *Cyber stalking: Challenges in regulating cyberstalking at the cyber space.* Legal Service India: http://www.legalserviceindia.com/legal/article-214-cyberstalking-challenges-in-regulating-cyberstalking-at-thecyber-space.html

Austin, J. (n.d.). *Stanford encyclopedia of philosophy*. https://plato.stanford.edu/entries/austin-john/#AnalJuriLegaPosi

Bocij, P. (2004). *Cyberstalking: Harassment in the internet age and how to protect your family.* Greenwood Publishing Group: www.praeger.com

Chahal, R. L. (2019). Cyber stalking technological form of sexual harassment. *International Journal on Emerging Technologies 10*(4), 367-73.

Citron, D. (2014). Hate crimes in cyberspace. Harvard University Press.

Citron, K. D. (2009). Cyber civil rights. *Boston University Law Review, 61*, 69–75.

Condry, R. I. (2010). Secondary victims and secondary victimization. In S. G. Shoham, P. Knepper, & M. Kett (Eds.), *International handbook of victimology.* (219–249). Boca Raton, FL: CRC Press,

Dhubey, N. Raman, V., Aggarwal, S. (2021, Jun. 2). India-social media rules 2021: Transforming social media. *Mondaq*.

Dooley, J. P. (2009). (2009). Cyberbullying versus face-to-face bullying: A theoretical and conceptual review. *Zeitschrift fur Psychologie / Journal of Psychology, 217*(4), 182-88.

Drebing, H., Bailer, J., Anders, A., Wagner, H., & Gallas, C. (2014). Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims. *Cyberpsychology, Behavior and Social Networking*, *17*(2), 61-7.

Duggal, P. (2009). *India's first cyber stalking case, some cyber law perspectives*. http://cyberlaws.net/cyberindia/2CYBER27.html

Ellison, L. & Akdeniz, Y. (1998, Dec.). Cyber-stalking: The regulation of harassment on the internet. *Criminal Law Review.* (Special issue), 29-48.

Ferdon, D. H. (2007). Electronic media, violence, and adolescents: An emerging public health problem. *Journal of Adolescent Health, 41*(1), 1-5.

Franks, M. A. (2010). Unwilling avatars: Idealism and discrimination in the cyberspace. *Columbia Journal of Gender and Law, 20*(2), 224-61.

Gokani, V. M. (n.d.). *Observations on the Proposed Amendments to the IT Act 2000*. ALAI. http://www.vijaymukhi.com/obsamend.doc

Groth, J. (2010). Cyberstalking – perspektywa psychologiczna. *Forum Oświatowe, 2*(1), 85-98.

Guide to Singapore's Protection from Harassment Act (POHA). (2022, Apr. 1). Singapore Legal Advice. https://singaporelegaladvice.com/law-articles/singapore-protection-harassment-act/

Halder, D. & Jaishankar, K. (2011). *Cyber crime and victimization of women: Laws, rights, and regulations.* Hershey, PA: IGI Global.

Hess, A. (2014, Jan. 6). Why women aren't welcome on the internet*. Pacific Standard.* https://psmag.com/why-women-aren-t-welcome-on-the-internet-aa21fdbc8d6

Holden, M. (2021, May 11). UK unveils law to fine social media firms which fail to reove online abuse. *Reutars.*

Hypś, S., Grześkowiak, A., & Wiak, K. (Eds). (2012). *Kodeks karny. Komentarz*. Wydawnictwo CH Beck.

Jaishankar, D. H. (2008). Cyber crimes against women in India: Problems, perspectives and solutions. *TMC Academy Journal, 3*(1), 48-62.

Jaishankar, D. H. (2011). Cyber gender harassment and secondary victimization: A comparative analysis of the United States, the UK, and India. *Victims & Offenders, 6*(4)*,* 386-98.

Jaishankar, K. (2005). Cyber stalking: A global menace in the information super highway. *ERCES Online Quarterly Review, 2*(3), 180-97.

James Rhodes v. OPO (By his litigation friend BHM), 2015 SCMR 1097 (Supreme Court of UK 2015).

Japan: Anti-Stalking Act. (2023). *Council of Europe*. https://www.coe.int/en/web/cyberviolence/-/japan-anti-stalking-act

Kashmiria, S. (2014). Mapping cyber crimes against women in India*. International Research Journal of Commerce and Law (IRJCL) , 1*(5), 22-38*.*

Keswani, M. H. (2017). Cyber-stalking: A critical analysis. *Bharati Law Review*, 131-48.

King-Ries, A. (2011). Teens, technology and cyberstalking: The domestic violence wave of the future. *Texas Journal of Women and the Law, 20*(2), 131-64.

Kosińska, J. (2008). Prawnokarna problematyka stalkingu. *Prokuratura i Prawo, 10,* 38-47.

Kyodo. (2017, Jan. 3). *Online stalking on social media becomes illegal in Japan*. SCMP. https://www.scmp.com/news/asia/east-asia/article/2058852/online-stalking-social-media-becomes-illegal-japan

Leyen, E. P. (2021, Jan 26). Special Address by President von der Leyen at the Davos Agenda Week. *European Commission Website.* https://ec.europa.eu/commission/presscorner/detail/en/speech_21_221

Lomba, N. (2020). Cyber Services Act*. European Parliamentary Research Service*.

Machanda, D., Kumar, P. R. (2021, Apr. 29). *The information technology (intermediary guidelines and digital media ethics code) rules, 2021: Impact on digital media*. Mondaq. https://www.mondaq.com/india/social-media/1063198/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021-impact-on-digital-media-?type=mondaqai&score=75

Mantilla, k. (2015). *Gendertrolling: How misogyny went viral.* Praeger.

Megarry, J. (2014). Online incivility or sexual harassment? Conceptualising women's experiences in the digital age. *Women's Studies International Forum, 47*(1), 46-55.

Nikolova, N. (2020). Japan's policy against the crime of Stalking. *Economics and Law 2*(1), 78-87.

Number of consultations related to stalker incidents in Japan from 2013 to 2022. (2023, Mar.). *Statista*. https://www.statista.com/statistics/865543/japan-number-stalking-

cases/#:~:text=In%202018%2C%20close%20to%2021.6,of%20the%20perpetrators%20were%20men

Pietkiewicz, M. & Trender, M. (2018). Cyberstalking in Social Media-Polish View. *Journal of Modern Science Tom, 38*(3), 29-40. DOI: 10.13166/jms/99217.

Powell, N. H. (2016). Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, Violence & Abuse, 19*(2), 195-208.

Sadotra, P. (2015). The technical and legal perspective of cyber stalking. *International Journal of Research Pedagogy and Technology in Education and Movement Sciences, 3*(3), 14-30.

Sakshi, M., Vashishth, A., & Teena. (2022). An analysis of cyber crime with special reference to cyber stalking. *Journal of Positive School Psychology, 6*(4), 1279-87.

Schwarzer, R. (2000). Manage stress at work through preventive and proactive coping. In E. A. Locke (Ed.), *The blackwell handbook of principles of organizational behavior* (342–55). Blackwell.

Shah, T. A. (2014). Indian women at risk in the cyber space: A conceptual model of reasons of victimization. *International Journal of Cyber Criminology, 8*(1), 57-67.

Shambhavee, H. M. (2019). Cyber-stalking: Threat to people or bane to technology. *International Journal of Trend in Scientific Research and Development (IJTSRD), 3*(2), 350-55 .

Sharma, N. (2021, Jun. 2). Social Media Rules 2021: Safety to Social Media. *Mondaq*.

Shimizu, A. (2013). Recent developments: Domestic violence in the digital age: Towards the creation of a comprehensive cyberstalking statute. *Berkeley Journal of Gender, Law & Justice, 28*(1), 117-37.

Siripala, T. (2022, Jul. 20). Japan toughens penalties for cyberbullying. *The Diplomat*. https://thediplomat.com/2022/07/japan-toughens-penalties-for-cyberbullying/

Śledziewski, D. (2013). Cyberstalking w polskim prawie karnym. In B. Hołyst, & J. Pomykała (Eds.), *Cyberprzestepczość i ochrona informacji. Bezpieczeństwo w Internecie.* Tom II" (red.) *Wydawnictwo Wyższej Szkoły Menedżerskiej, Warszawa*.

Sowalski R. M. (2010). Cyberprzemoc wśród dzieci i młodzieży, X-XII.

Spitzberg, C. (2007). The state of the art of stalking: Taking stock of the emerging literature. *Aggression and Violent Behavior, 12*(1), 64-86.

Tedx (Director). (2015). *Fighting for new laws to protect women in Japan* [Motion Picture].

Thapa, A. &. Kumar, R. (2011). Cyber stalking: Crime and challenge at the cyber space. *International Journal of Engineering Sciences, 4*(2), 340-54.

The Criminal Law (Amendment) Act. (2013). Extraordinary, The Gazette of India.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. (2021). PRS Legislative Research. https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021

Thelwall, M. (2002). Research dissemination and invocation on the web. *Online Information Review, 26*(6), 413-20.

Treder, M., Opalska-Kasprzak, A., (2016). Social media. Analiza prawnokarna I kryminologiczna. Zagadnienia wybrane. *Szczecin: Wydawnictwo Volumina.pl.*

Vitak, K. C. (2017). Identifying women's experiences with and strategies for mitigating negative effects of online harassment. *CSCW'17 proceedings of the 2017 ACM conference on computer supported cooperative work and social computing.* (1231-45). ACM.

Whitehead, T. (2011, Mar. 30). Just one in twelve suspected stalkers prosecuted. *Telegraph.*

Willard, N. (2006). *Cyberbullying and cyberthreats: Responding to the challenge of online social cruelty, threats, and distress.* Research Press.

Woodhouse, J. (2022, Mar. 15). *Regulating online harms*. House of Commons Library. https://commonslibrary.parliament.uk/research-briefings/cbp-8743/

World Economic Forum. (2021, Jan. 25) *The Davos Agenda.* World Economic Forum. https://www.weforum.org/events/the-davos-agenda-2021

Zarina, V. E. (2016). Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice*, *32,* 169-88.

Zygmunt Ł., & Trybus M., (2013). Aspekty kryminalistyczne, materialnoprawne i procesowe. *Rzeszów: Wydawnictwo Uniwersytetu Rzeszowskiego.*

Date of Publication	June 02, 2023