Received: May 02, 2024

Revised: May 23, 2024 & May 30, 2024

Published: June 15, 2024

Journal of Politics and International Studies
Vol. 10, No. 1, January–June 2024, pp.213–228

The intersection of technology and law: Challenges and opportunities in prosecuting cyberstalking cases in Australia and Pakistan

Muhammad Babar Shaheen
Lecturer, College of Law, Government College University, Faisalabad, Punjab, Pakistan
Corresponding: bsharal@yahoo.com

Muhammad Zahid
Advocate, District Courts Faisalabad, Punjab, Pakistan

Zaheer Ud Din Ahmad
Advocate High Court, District Bar Association, Pakistan

Abstract

The variety of offenses also changed with the development and progress of technologies in the world. There are a lot of benefits and paybacks of advanced modern technologies but at the same time, these technologies were used as a tool to commit an offense. After globalization, cybercrimes were introduced as a challenge for lawmakers and law enforcement agencies around the world. Cyberstalking is one of these modern and technical offenses. Cyberstalking is a form of online harassment through the use of electronic communication to attempt to threaten, portend, threaten, or harass another person. Such a threat or attempt to threaten causes fear and distress for the person repeatedly. Due to the day-by-day advancement of technology, this offense becoming popular among the masses. It has caused mental injury, depression, and anxiety among the victims and their families. Cyberstalking is a complex and intricate subject influenced by social behaviors, advanced technology, and laws.

This piece of research will elaborate on the definition of "cyberstalking", how this offense was committed, and what should be the effects on the victim's life. Furthermore, it explains the legal dimensions and social issues surrounding it in states like Australia and Pakistan. This research paper emphasizes existing laws, rules, and regulations adopted by both states and the importance of comprehensive approaches to effectively tackle cyberstalking, such as updating the existing laws, providing support services for victims, and raising public awareness.

Research reveals that both under-developed and developed states require public awareness, policies, and strict enforcement and execution of present laws to tackle and address cyberstalking. Both states need strong collaboration among legislative bodies, law enforcement agencies, internet service providers (ISPs), and community organizations to protect individuals in the digital world. In this regard, more research is required in both developed and developing countries.

Key Words: Cyberstalking, Legal Frameworks, Privacy Laws, Data Protection, Victim Support, Criminal Justice, Cyber Crime.

1. Introduction

Cyberstalking is an offense utilizing online harassment among other offenses through online means. It causes mental and psychological harm not only to its victims but also to their families in society. This kind of offense has no territorial limits and the impact or gravity of mental and psychological harm is more than any physical injury. By using electronic communication sources, the offenders create an atmosphere of threat and fear for victims and their families.

Cyberstalking includes sharing private photos or videos without permission, harassment on social media platforms, doxing, and intimating emails, online surveillance, and cyberbullying. (Cupach & Spitzberg, 2014). Such type of activities of the offender can lead to severe psychological distress as well as social isolation of the victims (Drebing et al., 2014). The legal framework against cyberstalking varies among developed and under-developing states (Vazquez & Jones, 2017). The main reason behind this is the financial issues of states.

States require effective and diverse tactics to overcome cyberstalking. These may include campaigns to educate and empower people, and public awareness campaigns (Bossler & Holt, 2020). States have to work on technological advancements to improve and counter cybersecurity and protect and prevent harassment (Khan, 2021). Furthermore, states effectively take cognizance to penalize such behaviors (Klein, 2019). To detect, investigate, and prevent cyberstalking instances, law enforcement institutions, internet providers, and social media platforms must work together (Sheridan & Grant, 2021). Despite obstacles, continuous initiatives are made to give victims justice and to make the internet a safer place (Khan, 2021).

2. Background of study

With 5.35 billion users as of January 2024, compared to only 16 million in 1995, the Internet has seen significant technological advancement and now serves 66.2% of the world's population (World Bank, 2024). Global connectedness was revolutionized by this surge, which was fueled by the World Wide Web and the Dot Com boom of the 1990s (Smith, 2018). The Apollo Guidance Computer is considerably behind other early computers in terms of speed (NASA, 2019). However, people are more concerned about security now than ever before due to greater connection (Fernandez, 2020). To secure personal data, advanced security procedures are required (Chen & Zhao, 2021).

The 1988 Morris worm incident demonstrates the range of motivations for cybercrime, from financial gain to personal fulfillment (Holt & Bossler, 2016; Shelton, 2018). Themes of hacking and the computational limitations of computers are frequently explored in science fiction (Smith & Johnson, 2016; Jones & Brown, 2019; Miller & Smith, 2017).

Global society is being reshaped by the internet's transformational potential, but it also presents issues like cybersecurity and digital literacy, which are essential for a secure, inclusive digital future (UNESCO, 2020).

2.1. Cyberspace Use in Pakistan

Merely 1% of Pakistan's populace made use of the internet in 1995. The country's digital transformation is reflected in internet adoption, which increased to 45.7% by the end of 2023, or 111 million users (Global Digital Reports, 2024). By January 2024, 71.7 million people, or 29.5% of the population, were active on social media platforms, indicating a rise in social media involvement (Global Digital Reports, 2024). With 188.9 million active connections representing 77.8% of the population mobile phone connectivity has greatly increased (Data Report, 2024).

In January 2024, there 242.8 million people were living in Pakistan; women made up 49.6% of the population and males 50.4% (Data Report, 2024). In addition, 38.2% of people resided in cities and 61.8% of people lived in rural areas. This gap between urban and rural areas emphasizes the necessity of focused initiatives to close the digital divide and guarantee fair access to digital resources for all populations.

2.2. Cyberspace Use in Australia

Australia's internet use in 1995 was 2.8%. It increased to 94.9% with 25.21 million users by early 2024, indicating a notable increase in digital connectivity (Global Digital Reports, 2024). Additionally, there was a rise in social media usage, with 20.80 million people, or 78.3% of the population, actively utilizing platforms (Global Digital Reports, 2024). 33.59 million active mobile connections, or 126.4% of the population, were attained in 2024, suggesting a widespread reliance on mobile technology.

January 2024 saw a 261,000 increase in Australia's population to 26.57 million, with women slightly outnumbering men (50.3% vs. 49.7%) (Data Report, 2024). 86.7% of Australians live in urban settings, underscoring the concentration of social and economic activity in metropolitan areas. The average age is 37.7 years, which highlights the necessity of appealing to a younger, tech-savvy population to spur digital innovation (Data Report, 2024).

3. Importance of Research

An important worldwide problem, cyberstalking is made worse by the widespread use of social media. Its alarmingly high incidence in Pakistan calls for an immediate

review of current policies and practices to better safeguard victims. Regulations that prohibit cyberstalking and impose fines for it exist, but they are mainly ineffectual. Effective study is now needed to assess Pakistan's legal system critically and offer significant, workable changes to fully address this problem.

The purpose of this research paper is to examine the cyberstalking legal systems in Australia and Pakistan, analyze the severity of cyberstalking at the moment in both nations, and determine how seriously the executive, judicial, and government branches are taking the issue. It will pinpoint any legal loopholes, examine case law for further clarification, and offer suggestions for improvements to victim protection. In addition, it will look at all applicable legislation and how well they protect victims.

More research is required to fully comprehend the correlation between age, ethnicity, and gender and the frequency of cyber victimization, as well as the psychological effects of these aspects. According to recent research, the government must be more proactive and make sure that laws are implemented correctly. A comprehensive study, however, is lacking in legislation that would make online stalking, especially against women and children, illegal and require state agencies to report, look into, and prosecute offenders. In conclusion, combating the cyberstalking epidemic necessitates a multifaceted strategy that includes strong legal reforms, efficient enforcement, and in-depth investigation to identify the sociodemographic elements that contribute to cyber victimization. The only way to successfully combat the growing threat of cyberstalking is to implement such measures.

4. Research Questions and Sub-Questions

1. How the legal frameworks in Pakistan and Australia address the issue of cyberstalking i.e., jurisdictional or cultural cases that involve cross-border elements.

4.1. Sub-Questions

1. What are the challenges and limitations in the existing legal frameworks in both countries in effectively addressing and preventing cyberstalking?

2. What are the differences and similarities in the legal remedies and penalties for cyberstalking in the two states?

2. Research objectives:

This research article's main objectives are to examine Pakistan's and Australia’s legal framework for cyberstalking, the current epidemic of cyberstalking in both states, the seriousness with which the government, courts, and executive branch are handling this problem and whether further action should be taken, where gaps in the framework exist, the analysis of cyberstalking case law for additional guidance, recommendations for changes and amendments to the framework, and an examination of all applicable laws and their relationship to victim protection.

To better understand the relationship between various criteria and the prevalence rates of cyber victimization, as well as how they affect the emotional repercussions experienced, more study on age, ethnicity, and gender needs to be done.

Researchers have generally advised that the government should take a more active role and that laws should be implemented effectively. However, no effective research has been done to propose legislation that would make it illegal to stalk people online, particularly women and children, and that would require the state apparatus to report, investigate, and prosecute any such offenders.

3. Literature Review

Cyberstalking, a pervasive menace, particularly targets women, engendering an environment fraught with gender-based harassment and violence. The tactics employed in cyberstalking often extend beyond mere digital intrusions, encompassing threats of physical harm, sexual violence, and the malicious dissemination of private information, including intimate images and videos. The profound psychological and emotional toll exacted upon victims underscores the urgent imperative for robust interventions and legislative measures aimed at combatting this insidious form of gender-based violence (Digital Rights Foundation, 2012).

Despite the ever-evolving landscape of online platforms and digital communication channels, Facebook remains a central locus of reported online harassment, with a staggering 45% of callers to DRF's Helpline citing experiences of harassment on this platform. The insidious manifestations of cyber harassment encountered by victims encompass a range of egregious behaviors, including blackmail, unsolicited messages, the unauthorized use of personal information, and the proliferation of fraudulent profiles. While DRF diligently collects information from callers with utmost respect for their privacy and confidentiality, the organization is cognizant of prevailing challenges, such as callers' apprehensions regarding location sharing, with Punjab emerging as a focal point, representing 50% of Helpline callers (Digital Rights Foundation, 2012).

6.1. Existing Research on Cyberstalking Prosecution

Many previous studies conducted on the prosecution of cyberstalking provide insight into the challenges and strategies that are involved in lawfully addressing this form of online harassment. Upon investigation of this research, several key themes were revealed.

According to Dawn News, cyberstalking represents one of the most prevalent cybercrimes, encompassing a range of offenses from financial fraud to website hacking. Over 80% of grievances reported to the Federal Investigation Agency (FIA) involve cyberstalking, primarily targeting young women with extortion, harassment, and blackmail (Dawn News, n.d.). Victims often face challenges in

reporting incidents due to a lack of awareness about the reporting process (Dawn News, n.d.).

On May 18, 2023, the Digital Rights Foundation (DRF) released its sixth annual Cyber Harassment Helpline Report for 2022, documenting 14,376 reported cases over the past six years. In 2022 alone, the helpline received an average of 224 new cases per month, with November 2022 being particularly busy (Digital Rights Foundation, 2023).

Many studies support improvements to the law that would reinforce prosecutorial control and anti-cyberstalking legislation. This may mean creating strategies to discourse current developing forms of online abuse and harassment, imposing penalties for offenders, and extending the understanding of cyberstalking.

More research in this area is still needed to identify best practices, measure the impact of legislative changes, and implement practical counterstrategies for cyberstalking in a dynamic digital context.

6.2. Technological Advancements and Their Impact on Cyberstalking Investigations

Technological advancements played a significant role and had a great influence on cyberstalking investigations, both facilitating and posing new challenges for law enforcement. Using digital platforms and various gadgets has greatly increased the potential evidence in cyberstalking cases.

Due to vast technology, law enforcement agencies can gather a wide range of digital evidence that includes emails, metadata, GPS data, social media posts, and instant conversations, that support these cases. The collected digital data, its storage, and analysis are still a challenge for these agencies not only due to huge quantity and variety but also due to lack of resources and experience.

By using modern forensics tools and techniques, the investigating agencies are now on better footing to analyze and locate digital indicators across a variety of social media platforms and different devices. After using advanced tools and techniques the investigation agencies recover deleted data or information, monitor the online activities of offenders, and connect digital artifacts to specific offenders. It is also challenging for law enforcement agencies to stay up to date with the rapid improvements in technology, and forensic procedures. The states are required to train officers and officials of investigating agencies regularly about the latest forensic techniques.

6.3. Cultural and Social Factors Influencing Cyberstalking Reporting and Prosecution

Penalties and reports that are associated with cyberstalking are greatly impacted by cultural norms and society. In many communities, victims due to adverse cultural and sociological concerns did not report and so criminals were never punished. In many communities, it is considered stigmatizing to be the target of cyberstalking, particularly when the harassment involves very sensitive or private information.

Some victims may be too humiliated or feel ashamed to report the abuse because they fear rejection or unfavorable social repercussions.

Some victims may be concerned about the receiving of adequate assistance and protection from law enforcement departments, or they may be fearful of the perpetrators taking revenge on them.

The general views about technology, privacy, and interpersonal connections usually vary among different cultures, which could influence how an individual regards cyberstalking behavior. The restrictions between appropriate online harassment and online behavior might not be as well-known or irritating in societies whose everyday life is mostly powered by digital communication.

6.4. Overview of Cyberstalking Laws in Australia and Pakistan

Both Pakistan and Australia have taken practical steps by enforcing laws and regulations to control cyberstalking and other forms of online harassment. These legal frameworks provide significant progress in identifying and addressing the difficulties of cyber threats in the digital age. However, despite these efforts, many challenges persist in effectively implementing these laws and providing complete support and guidance to victims of cyberstalking.

The Prevention of Electronic Crimes Act, (PECA) 2016 is the latest legislation on cybercrime protection and penalization in Pakistan. The Federal Investigation Agency (FIA) works as an investigating agency under the above-said statute and the investigation of cyberstalking was assigned to its wing known as the Cyber Crime Wing (CCW). The establishment of this specialized unit occurred in 2007 to identify and combat technological abuse within society (Federal Investigation Agency, n.d.).

The Electronic Transactions Ordinance was enforced by Gen. Musharaf as President of Pakistan in the year 2002. This law serves as a primary law concerning cybercrime in Pakistan, originally focusing on facilitating file handling, statistics, communications, and transactions. However, its scope expanded to include certification agencies and virtual format authentication (Electronic Transactions Ordinance, 2002).

Under PECA 2016, cyberstalking is defined as the intentional use of an information system, network, website, email, or similar communication method to intimidate, coerce, or harass another individual (Prevention of Electronic Crimes Act, 2016).

The CCW of the FIA, established in 2007, plays a crucial role in investigating and prosecuting cybercrimes in Pakistan. Tasked with enforcing the laws outlined in PECA 2016, the CCW focuses on addressing a wide range of cyber threats, including cyberstalking. Through its specialized training and expertise, the CCW is equipped to handle complex cyber investigations and gather evidence against cyber criminals (Federal Investigation Agency, n.d.).

There are various laws in Australia for cyberbullying like using a phone or the internet menacingly, stalking, making threats, encouraging suicide, posting nude offensive images, etc. Despite these laws rate of cybercrimes is not controllable.

7. Legal Frameworks

The laws in Australia and Pakistan related to cyberstalking and online harassment reflect the growing recognition of the seriousness of these offenses and the need for legal frameworks to address them. Here's a review of the laws in both countries:

7.1. Australia:

7.1.1. Criminal Code Act 1995

This federal legislation includes provisions related to cyberstalking, such as stalking offenses that encompass electronic communication. It criminalizes behaviors intended to cause fear or harm through repeated communication or surveillance.

7.1.2. Telecommunications Act 1997

The Telecommunication Act 1997 was enforced to deal with different aspects of telecommunication in Australia. It contains provisions relating to misuse of telecommunication networks for stalking or harassment purposes.

In Australia, besides the federal laws each Australian state and territory has its laws and policies regarding cybercrimes including cyberstalking. For instance, the states of New South Wales, Victoria, and Queensland have approved laws that proscribe stalker behavior, as well as cyberstalking, under their Crimes Acts or Criminal Codes respectively.

7.1.3. Civil Remedies:

The legal system of Australia also allows civil remedies to victims in cyberstalking cases along with criminal prosecution keeping in view the concept of fair trial. These civil remedies include mandatory and perpetual injunctions or restraining orders against the offender. Another form of civil remedy includes damages against the wrongdoer.

7.1.4. Cyber Law Enforcement Agencies:

Australia’s federal, state, and territory law enforcement agencies investigate and prosecute cyberstalking offenses. These agencies work together to prevent and penalize cybercrimes including cyberstalking by collecting data for evidence, supporting victims, and pursuing legal measures against offenders. States like Australia have a strong and effective civil and criminal justice system. However, due to the advancement of modern technologies, offenders use the most advanced techniques and tools to commit online crimes, and law enforcement agencies face new challenges in this way to overcome these offenses.

As day-by-day technologies are going to advance, the Australian government needs to strengthen the procedural laws and the law enforcement agencies through

refresher courses, training their staff with the use of the latest technology, and raising public awareness and knowledge in society. The role of NGOs in this regard is also a need of the day.

7.2. Pakistan:

FIA is the agency empowered under the Prevention of Electronic Crimes Act, 2016 (PECA) to investigate and submit challan before a special Central Court about offenses relating to cybercrime including cyberstalking. The special court proceeded with the trial as provided under the provision of the Code of Criminal Procedure, 1898. And victims as well as the offenders have the right to appeal before higher courts as provided by the Criminal Code. The victim and his/her witness have protection under the law throughout the trial proceedings.

7.2.1. The Prevention of Electronic Crimes Act, 2016

The main objectives of this act are to regulate electronic communication and eradicate cybercrime including harassment, terrorization, and stalking. PECA proscribes different activities, including spreading false information, engaging in cyberstalking, harassing people online, or gaining unauthorized access to information systems of victims' accounts including individuals and organizations. It also provides a variety of legal tools to investigate and prosecute cybercrimes, as well as protocols for the preservation and admissibility of electronic evidence in court processes.

7.2.2. The Pakistan Penal Code, 1860

Even though the PPC was implemented before PECA and was primarily intended to address conventional crimes, its provisions are irregularly used with PECA to prosecute cyber stalkers. Incidents of Cyberstalking are sometimes subject to the PPC's provisions on offenses like intimidation, harassment, and defamation.

There are some other laws apart from the PPC and PECA, that have provisions in Pakistan that might also affect cyberstalking occurrences. These laws include dealing such as telecommunications, data protection, and privacy rights, these laws impact the investigation and prosecution of cyberstalking crimes.

7.3. Comparison of Both Legal Frameworks and Effectiveness:

During the comparative study of Australian and Pakistani legal system many factors were considered. It is a fact that Australia has an inclusive legal system with the latest technology to control online offenses including cyberstalking. The Pakistani legal system countering the online offences like cyberstalking requires effecting and practical amendments along with improvements in use of advance technologies to investigate and prosecute the offenders.

Australia has a strong investigation, prosecution and judicial system which provides not only effective remedies to victim after commission of offence but also protect society from committing of any cybercrime.

On the other hands, due to lack of resources, technical limitations, and institutional competence, the legal system in Pakistan dealing the cybercrimes is not effective one. Australia has made great efforts to educate the public about cyberstalking and to provide victims with help and information till the decision of the case. Pakistan is required to launch awareness campaigns and educational activities at the national level about cyberstalking. The National and International NGOs have to focus on this particular offence along with Federal and Provincial Governments.

Both Pakistan and Australia have legal frameworks to counter cyberstalking but due to advanced technologies, well-trained law enforcement agencies, the latest investigating tools, and well aware society, Australia's approach may be more effective and robust.

It is need of the day that Pakistan can counter cyberstalking through bolstering its enforcement mechanisms, strengthening its legal framework and increasing public awareness in order to combat cyberstalking and protect people's digital rights and safety.

7.4. Technological Advancements

The methods to investigate offenders of cybercrimes have changed in the past decade due to scientific and technological advancements. Some of the scientific and technological advancements are as follows.

- Now the deleted data can be recovered. The online activities of suspected persons can be monitored. The digital and forensic methods help investigation agencies to identify the offenders of cyberstalking by collecting, reviewing, and evaluating electronic evidence from different digital devices.
- Different analytics tools and firewalls are available to analyze messages, conversations, and posts on social media platforms, and to track, help, and evaluate data, revealing links, patterns, and trends in case of offenses of cyberstalking.
- The ability to collect and preserve digital evidence from online platforms is made possible by advancements in online evidence collection and preservation.
- By automating the archiving of webpages, chat logs, and screenshots, investigators may ensure the integrity and admissibility of their evidence in court.
- The laws relating to the admissibility of evidence are amended by both states to admit evidence collected from modern devices

8. Benefits, Limitations, and Challenges in Prosecuting Cyberstalking Cases

8.1. Benefits:

The collection of online evidence, social media analytics, and technological advancements are a great milestone to achieve effective cyberstalking investigations. Social media analytics help to increase ability to monitor and trace the behavior of suspects more efficiently and accurately. The advanced technologies are also helpful in gathering evidence and have simpler access to digital evidence from several web sources.

8.2. Limitations:

Even though there are many benefits and advantages to the use of modern techniques and technologies in cyberstalking investigations but there are also many drawbacks as well. The drawbacks may include privacy issues, legal restrictions on digital evidence, and managing massive amounts of digital data. These techniques and tools need expertise as well as specific training. Another major drawback is territorial jurisdiction and collection of data when the offender uses a server beyond the jurisdiction of his state.

8.3. Challenges

Both states face many challenges to penalize, prevent, and eliminate cyberstalking from their societies. It is very important to pinpoint and examine the major challenges to counter cyberstalking and to develop effective policies and strategies to overcome this type of harassment. Here are some key challenges that are faced by both countries.

- Many victims of cyberstalking victims hesitate to report incidents due to fear of retaliation, embarrassment, or the belief that law enforcement cannot effectively address the issue. As a result, many cases go unreported and offenders get liberty of this situation which may lead to committing the same offense again and again. Furthermore, it leads to unavailability or lack of accurate data.
- Due to rapid technological advancements like; anonymization tools, encryption techniques, and social media platforms, make it challenging for law enforcement agencies to track and identify offenders.
- Cyberstalking cases are frequently involving offenders and victims located in different jurisdictions, both domestically and internationally. The jurisdictional boundaries; and extradition processes complicate the investigations and prosecutions. In other words, it is impossible to penalize such an offender.
- The definitions and punishments of cyberstalking vary in different states which results in creating legal gaps and inconsistencies among the masses particularly in cases when the offenders use the cyberspace of any other state.

- In developing states, law enforcement agencies often face constraints on resources, including limited funding, staffing shortages, and inadequate training in cybercrime investigation techniques.
- Many victims of cyberstalking lack access to adequate support services and resources. Additionally, there may be a lack of awareness among law enforcement, policymakers, and the general public about the prevalence and impact of cyberstalking, further marginalizing victims and impeding efforts to address the issue.
- Societal attitudes towards gender-based violence, online harassment, and blaming of victims can influence how cyberstalking cases are perceived and addressed.
- Promoting digital literacy and providing awareness of online safety practices is very essential for preventing cyberstalking and empowering individuals to protect themselves online from cyberstalking.

9. Opportunities for Improvement

There are various opportunities for enhancement to surmount the previously listed challenges and enhance the prosecution of cyberstalking cases:

9.1. International Cooperation:

Investigating and prosecuting cyberstalking crimes can be made easier by strengthening cross-border cooperation between law enforcement agencies through formal information-sharing channels, mutual legal aid treaties, and joint task forces.

9.2. Investing in Specialist Cybercrime Units and Improved Training:

Digital forensics and cyber investigations can improve law enforcement's capacity to locate and detain online criminals as well as collect digital evidence.

9.3. Public Education Initiatives:

By raising public knowledge of the risks of cyberstalking, online harassment, and safe online behavior, victims may be more likely to come forward with reports and ask for assistance.

9.4. Legal Reforms and Updates:

Improvements in the legal frameworks for the prosecution of cyberstalking cases and updating and broadening the existing laws to overcome and evaluate the new cyber threats can enhance the enforcement of rules and laws. Cooperation across borders is facilitated by harmonizing legislation with the help of international norms. Policymakers, law enforcement, and community stakeholders can increase the layer of protection of persons from online abuse and harassment by putting these steps into action.

10. Successful prosecution Strategies

10.1. Successful Prosecution Strategies Adopted by Australia

Government agencies are involved in conducting a digital forensic analysis thoroughly by using IP addresses that involve harassment and cyberstalking. All departments collaborate with departments to obtain information on the accounts of users; officials also collaborate with social media companies to track out the harassing accounts' owners. After that during case proceedings, victim advocacy groups and attorneys assisted the victim by documenting the harassment, tracking down relevant evidence, and providing emotional support.

10.1.2. Challenges Faced by Australia:

To escape from detection, many criminals often use anonymous software to mask their identities, sometimes making it difficult for law authorities to track such criminals down and apprehend them.

10.2. Successful Prosecution Strategies Adopted by Pakistan:

10.2.1. Jurisdiction Concerns:

Many cyberstalking cases related to social media platforms and foreign offenders need to address matters that need cooperation between law enforcement organizations in various jurisdictions.

10.2.2. Anonymity of Perpetrator:

Most of the Criminals frequently hide their identities and use anonymity software to avoid identifying and arresting, which makes it more challenging for law enforcement authorities to find and arrest them.

10.2.3. Evidence Collection:

For cyberstalking trials, digital evidence from social networking sites is very essential. For evidence collection specialized skills and techniques are required to ensure the authenticity and collection of evidence of the crime.

10.2.4. Challenges Faced by Pakistan:

10.2.4.1. Cultural Barriers:

Victims of cyberstalking may face cultural barriers that can prevent them from reporting the harassment or restrain them from law enforcement due to social stigma or fear of retaliation. It is a very common issue in Pakistan.

10.2.4.2. Lack of Awareness:

Most of the victims are unaware of their rights regarding cyberstalking or they simply don’t know where and how to report the crime. That’s why it is very difficult to eliminate it.

10.2.4.3. Technological Difficulties:

With the speed at which technology and encryption methods are developing, law enforcement agencies have trouble locating harassing message sources and compiling digital evidence.

11. Conclusion

There are a lot of communal problems and areas for improvement when comparing cyberstalking prosecutions in Pakistan and Australia. Both countries face difficulties with jurisdiction, privacy, and evidence collection when pursuing cyberstalking prosecutions. To overcome these challenges, there should be some improvements in the existing system that can encourage victims to take action against cyberstalking. However, some cases are currently resolved by employing successful prosecution strategies such as digital forensic analysis, victim assistance programs, and specialized cybercrime units.

12. Recommendations for Improving Cyberstalking Prosecution

- **Improved International Cooperation:**

  The enhancement in cross-border law enforcement agencies' cooperation to enable the exchange of information and cooperative investigations of cyberstalking involving foreign offenders can bring fruitful results.

- **Public Awareness Campaigns:**

  Raising public awareness about cyberstalking legislation, victim assistance, and reporting procedures to encourage reporting and discourage cyberbullying.

- **Legal Reforms:**

  Implementation of more protective and updated Laws and ensuring the implementation of legislation can address emerging threats. Legal reforms are more important to implement to ensure protection for victims of cyberstalking.

- **Technological Advancements:**

  Investing more funds in this sector to generate advanced mechanisms and advanced technology could be an initiative to overcome cyberstalking as it will improve the methods of investigation and make victims more secure.

- **Victim-Centric Approach:**

  Both states must assign funds for victim protection and support services, such as therapy, legal help, and privacy safeguards, to lessen the psychological and emotional effects of cyberstalking occurrences.

References

[1] Australian Bureau of Statistics (ABS).

[2] Byrne, Sean, and Jessica Senehi. 2012. Violence: Analysis, Intervention, and Prevention. Athens: Ohio University Press.

[3] C Zhao, H Guo, J Li, T Myint, W Pittman, L Yang, W Zhong, RJ Schwartz, Development 141 (2), 281-295.

[4] Cavezza, C., & McEwan, T. E. (2014). Understanding cyberstalking: Prevalence, motivation, and victim impact. *Journal of Cybersecurity Education, Research and Practice*, 2014(1), 17-28.

[5] Chan, C.-H. (2011). Reconceptualizing the mechanism of Internet human flesh search: A review of the literature, 2011 International Conference on Advances in Social Networks Analysis and Mining (ASONAM) (pp.650-655). Kaohsiung, Taiwan: IEEE.

[6] Chaudhy, S. (2011). The rise of cybercrime in Pakistan: Challenges and solutions. *International Journal of Cyber Law*, *5*(2), 112-125.

[7] Crimes Act 1914 (Cth).

[8] Crimes Act 1995 (Cth) Div 473.1 amended by (Telecommunications Offences and Other Measures) Act 2004 (Cth).

[9] Criminal Code Act 1995 (Cth) (Australia).

[10] Criminal Code Act 1995 (Cth) amended by Criminal Code Amendment (Theft, Fraud, Bribery & Related Offence Act) 2000 (Cth) div 133 (1).

[11] Criminal Law Consolidation Act 1935 (SA).

[12] Cupach, William & Spitzberg, Brian (2007). The State of the Art of Stalking: Taking Stock of the Emerging Literature. Aggression and Violent Behavior. 12. 64-86. 10.1016/j.avb.2006.05.001.

[13] Cybercrime Act 2001 (Cth) div 476(1).

[14] Dreßing. Maple, Carsten (2014). The impact of cyberstalking: The lived experience - A thematic analysis-

[15] Fernandez, Pablo and de Apellániz, Eduardo and F. Acín, Javier, Survey: Market Risk Premium and Risk-Free Rate used for 81 countries in 2020 (March 25, 2020). IESE Business School Working Paper No. WP-1244-E, Available at

[16] Finn, Jerry. 2004. A survey of online harassment at a university campus. *Journal of Interpersonal Violence* 19: 468–83.

[17] Holt, Thomas & Bossler, Adam. (2014). An Assessment of the Current State of Cybercrime Scholarship. Deviant Behavior.

[18] https://www.dawn.com/news/1078417

[19] https://www.pandasecurity.com/en/mediacenter/types-of-cybercrime/

[20] Johnson, L., & Brown, R. (2018). Victim support services for cyberstalking victims: An exploratory study. *Journal of Interpersonal Violence*, 33(5), 821-844.

[21] Khan, E. A. (2022). Manual of Cyber Crimes. Lahore: *Insaf Law House*

[22] Khan, M. (2021). The digital landscape of Pakistan: Trends and challenges. *Pakistan Journal of Technology*, 12(2), 67-82.

[23] Prevention of Electronic Crimes Act. (2016). Pakistan.

[24] Protection from Harassment Act 1997, c. 40 (UK).

[25] Sheridan, Lorraine P., and Tim Grant. 2007. Is cyberstalking different? *Psychology, Crime & Law* 13: 627–40.

[26] Sheridan, Lorraine P., and Tim Grant. 2007. Is cyberstalking different? *Psychology, Crime & Law* 13: 627–40.

[27] Sheridan, Lorraine, Raphael Gillett, and Graham Davies. 2002. Perceptions and prevalence of stalking in a male sample. *Psychology, Crime and Law* 8: 289–310.

[28] Smith, J. (2020). Cyberstalking: Understanding the phenomenon and its consequences. *Journal of Cybersecurity*, *5*(2), 123-145.

[29] Smith, J. (2021). Privacy and data protection laws in Australia. *Journal of Cybersecurity*, *10*(2), 45-58.

[30] Smith, L. (2022). Digital trends in Australia: Insights and implications. *Australian Journal of Technology*, *35*(1), 45-58.

[31] Vasquez, Vivian. (2004). Negotiating Critical Literacies with Young Children. Negotiating Critical Literacies with Young Children.