**The Lighthouse Journal of Social Sciences, Vol. 03, Issue 2, Winter 2024, pp. 1-13**

# Cyberstalking Legal Frameworks in the Digital Age: A Comparative Analysis of the United Kingdom, United States of America and Pakistan

**Johar Wajahat[1], Marghzar Tarana[2], Seema Gul[3]**


## ABSTRACT

*Cyberstalking has become one of the most communal subjects in the digital world, creating a pressing need for sound legal frameworks to address its complexities and mitigate harm to victims. This research conducts a comparative analysis of cyberstalking laws in the United States, the United Kingdom, and Pakistan to evaluate the efficacy, scope, and enforcement of existing legislation. In the United States, federal and state laws, such as the Interstate Communications Act of 2012 and the Protection from Harassment Act, address various aspects of cyberstalking, including harassment, threats, and extortion. Similarly, the United Kingdom's Protection of Freedoms Act 2012 and Online Safety Act 2023 provide a more advanced framework, with provisions for both minor and severe offenses, focusing on accountability. On the other hand, Pakistan's Prevention of Electronic Crimes Act (PECA) 2016 barely covers cyberstalking issues and primarily deals with the misuse of electronic communication. This study highlights the critical gaps in Pakistan's legal structure and analyzes how legislation developed in the United States and the United Kingdom could inform reforms. By emphasizing international best practices, this research aims to contribute toward creating more comprehensive cyberstalking laws in Pakistan that enhance victim protection and align with global standards.*


***Keywords:*** *Cyberstalking, legal structural frame, accountability, online platforms, critical gaps & global concerns*

## INTRODUCTION

Cyberstalking has arisen as a gigantic matter in today's world, with technological improvements directly contributing to an increase in such crimes. Electronic media is quickly becoming one of the chief technologies of our day. Our culture is increasingly reliant on technological breakthroughs to access information globally. While this has many advantages, it also has certain drawbacks, especially in terms of personal privacy and the growing problem of cyberstalking. This research provides an outline of unanticipated actions such as privacy problems,

[1] Assistant Professor, Department of Law, Shaheed Benazir Bhutto Women University Peshawar
**Corresponding Author's Email:** johar.wajahat@sbbwu.edu.pk
[2] Lawyer/Associate, Kakakhel Law Associates, Peshawar District Court, Khyber Pakhtunkhwa
[3] Assistant Professor, Law College, University of Peshawar, Khyber Pakhtunkhwa

Manuscript Submitted: November 25, 2024
Manuscript Accepted: December 10, 2024

cyberstalking, and cyber harassment in Pakistan. It also examines tactics for combating cyberstalking offenses, legal procedures, and preventative recommendations to mitigate this global problem. Cyberstalking is the activity of utilizing technology, primarily the Internet, to cause dread or anxiety in another person regarding their safety (Fisher, 2002). An ample definition of stalking is a persistent pattern of behavior in which one person intrudes on another's personal life in a way that is seen as treacherous. This behavior manifests as a pattern of repeated activities over time, which is threatening and generally frightening, and it violates a person's right to privacy (Spitzberg & Hoobler, 2002). The general use of digital technology and the Internet has created a very suitable environment for cyberstalking, which affects a huge total of people, mostly women around the world. Despite the recent passage of several cybercrime laws, which are ostensibly intended to combat all types of cybercrime, including cyberstalking, substantial issues about their practical implementation and effectiveness, persist. In this regard, it remains to be observed how far these laws have progressed in addressing cyberstalking by analyzing judicial outcomes, and whether there are still gaps in the current legal framework. This research will also compare Pakistan's cyberstalking legislation to the United States and the United Kingdom as technologically developed countries in order to identify gaps and learn from international best practices. To analyze and compare the legislative provisions addressing cyberstalking in the USA, UK, and Pakistan, focusing on their scope, penalties, and enforcement mechanisms.

**Research Questions**

The study highlights the factors related to:

i. The legislative frameworks and how they differ in their approach to defining and addressing cyberstalking in the USA, UK, and Pakistan?
ii. The key challenges in enforcing cyberstalking laws in Pakistan compared to the USA and the UK.

## LITERATURE REVIEW

Any crime that employs a computer as a tool, target, or means is referred to as cybercrime, a word that was created in recent years. Cybercrimes mostly target the data of individuals, groups, communities, or governments. (Shambhavee, 2019). A form of cyberbullying known as "cyberstalking" entails malicious, persistent, and targeted online conduct. Cyberstalking is defined in a variety of ways, but generally speaking, it refers to persistent, deliberate attempts to utilize technology to threaten, intimidate, or control someone. (Haq & Zarkoon, 2023).Important characteristics include utilizing social media, email, and other online channels to cause psychological harm, violate privacy, or damage the victim's reputation. (Wilson et al., 2022)

This literature review explores cyberstalking laws in Pakistan, delving into a comparison of Pakistan's legal framework with the approaches of the USA and the UK. Section 24 of Pakistan's Prevention of Electronic Crimes Act (PECA) 2016 establishes the legal framework for handling cyberstalking and other types of harassment. The statute stipulates that individuals found guilty of cyberstalking face a fine or up to three years in prison. Threats, harassment, and unlawful access to personal information are among the offenses covered by the Act.

The PECA 2016 Act's shortcomings, according to critics, include being ambiguous and potentially unenforceable, which could cause more harm than good if it doesn't provide protection for those who need it the most. A thorough examination of PECA 2016 shows that it contains a clause pertaining to cyberstalking. The dissemination of pornographic material, harassment, and the misuse of electronic information are all expressly prohibited by Section 24 of the PECA 2016 (PECA, 2016). Despite these developments, the research that is currently available shows conflicting findings about PECA 2016's efficacy. According to studies, although the law offers a strong structure, procedural difficulties, a lack of awareness, and a lack of resources cause its enforcement to be uneven. (Saleem, 2022) Moreover, while the necessity of international collaboration to harmonize legislation and investigative methods is becoming more widely acknowledged, the transnational nature of electronic communications creates jurisdictional challenges. The United States, the United Kingdom, and other larger, more technologically sophisticated nations have made cyberstalking a crime (Chik, 2008).

In the US, stalking both traditional and cyber has grown to be a serious social and legal problem. Research shows that whereas stalking victimization receives a lot of attention, little is known about cyberstalking victimization in particular. A study comparing stalking victimization among university students in Spain and the United States emphasizes how crucial it is to look at these problems in various national contexts to comprehend their nature and prevalence. (Cruz, 2021).

The USA has created a thorough legal structure, including federal and state-level regulations, to combat both traditional and cyberstalking in spite of these obstacles. For example, cyberstalking is particularly addressed under California Penal Code Section § 646.9, which gives authorities a legal foundation to prosecute violators. (California Penal Code, 1872). A key strength of the UK framework is the immediate provision for Stalking Protection Orders (SPO), which allow victims to apply for protection without resorting to criminal sanctions. The Protection from Harassment Act 1997, which was later further updated and modified by the Malicious Communications Act 2003 and the Stalking Protection Act 2019, is an example of the UK's approach to cyberstalking. These laws include provisions for punishing individuals who engage in repeated, unwanted online communications that cause distress, fear, and other contributing elements (Stalking Protection Act 2019).In the UK, the widespread use of connected devices has fundamentally altered how individuals interact with information, systems, and one another in society, particularly among young people who are frequently referred to as "digital natives." Although technology has greatly improved our lives, it has also enabled certain people to engage in harmful behaviors against others, such as cyberstalking. The nature of these online assaults, the relationships between the victim and the perpetrator, and the technological and legal frameworks that have responded to this new situation have all been covered in the literature. The findings of these studies lend credence to the idea that in order to combat cyberstalking and shield people from online harassment, legal and technological frameworks must cooperate (Maple, 2012).

Cyberstalking is a very complex and multifaceted crime, and while Pakistan has made progress in this area since the Prevention of Electronic Crimes Act (PECA) was passed in 2016, there is still much space for improvement in terms of enforcement and preventative measures. In contrast, the United States and the United Kingdom have more advanced criminal laws and legal

procedures to prevent and generally improve the problem. These could be crucial models for Pakistan when it comes to specific law changes pertaining to cyberstalking. Pakistan may improve its capacity to protect its citizens in the digital age by fortifying its laws, guaranteeing more efficient enforcement, and collaborating with other countries.

## RESEARCH METHODOLOGY

This study employs a qualitative legal research methodology, through comparative legal analysis, to study the definitions, criminalization, and legal measures taken against cyberstalking in Pakistan's, the United Kingdom's, and the United States' legal context. The research offers a critical analysis of the legislative provisions and enforcement techniques governing cyberstalking in these jurisdictions, with a view to determining legal loopholes, strengths, and areas requiring reform, particularly for Pakistan.

The main sources of this study are laws like the Protection from Harassment Act 1997 and the Online Safety Act 2023 in the UK, the Interstate Communications Act 2012 and state laws in the USA, and relevant laws that are presently in force in Pakistan, such as the Prevention of Electronic Crimes Act 2016. Secondary sources include journal articles, academic analysis, government reports, and data from legal databases such as HeinOnline, JSTOR, Westlaw, and government websites. These resources provide in-depth information on the development, extent, and implementation of cyberstalking laws.

The comparative framework of the study is structured on specific parameters, namely the statutory definition of cyberstalking, the legislative definitions, the categories and level of punishment, the procedural protections, and the quality of assistance provided to the victims through these laws.

This facilitates a rational comparison of how well each legal framework tackles cyberstalking and supports the drawing of conclusions about their relative advantages.

### Evaluating Cyberstalking under Pakistan's Cyber Laws

Examining the legal framework in Pakistan on cyberstalking under the different laws demonstrates how much each law coup with the delinquent of cyberstalking: The regulation and management of telecommunication services are the main emphasis of the Pakistan Telecommunication (Re-Organization) Act, 1996 and the Telegraph Act, 1885. Their policies on modern digital hazards, such as cyberstalking, are out of date. Victims of cyberstalking have no legal recourse because current laws no longer cover the modern meaning or concepts of internet harassment. Instead of focusing on specific cybercrimes, the Electronic Transaction Ordinance of 2002 and the National Information Technology Policy and Action Plan of 2000 prioritize expanding IT infrastructure and enshrining electronic transactions in law. These steps lay the groundwork for digital commerce and IT progress, but they do not directly address cyberstalking or its victims. The Electronic Crimes Act of 2004 began the process of dealing with cybercrime in general, but it did not address specific issues such as cyberstalking. Despite providing a broad foundation for electronic crimes, it lacked particular regulations addressing online harassment and

stalking. The Cyber Security Council Bill, 2014, offered improvements to cyber security measures but made no particular mention of the problem of cyberstalking. While the Bill addressed more basic cyber security issues, it fell short of providing a sufficient legal response to cyberstalking. The Prevention of Electronic Crimes Act, 2016, also known as PECA, is a new legal tool to combat the growing phenomenon of cyberstalking, which is defined as "the intentional use of electronic communication equipment for purposes of affecting, disturbing, harassing, among other things, to another person." Section 24 of the PECA defines cyberstalking as using an information network, a website, email, or other comparable communication channels to harass, threaten, or coerce another person. The Federal Investigation Agency Act of 1974 refers to the FIA's investigative power but does not offer specific legislative guidelines for cyberstalking. This is persistently attempting to contact or follow someone, even in the event that they do not reply or express any interest. Cyberstalking also includes the practice of keeping an eye on someone's internet, instant messaging, email, or other electronic communications in a way that causes them to feel uncomfortable, scared, or disturbed. Another offense is cyberstalking, which is when someone takes another person's photos or videos without that person's consent and shares them in a way that hurts that person. Violations of this clause can also result in fines of up to one million rupees, more than three years in jail, or both. Furthermore, if the victim is a minor, punishments of up to five years in jail and/or fines of 10 million rupees may be imposed.

Additionally, the legislation allows victims or a minor's legal guardians to request through a complaint that damaging data be banned, erased, or taken in any other way; in such a scenario, the authorities are required to take immediate action. PECA closes the previously unresolved legal gap by specifically addressing the issue of electronic harassment and offering practical solutions to combat it. In hindsight, PECA provides the most pertinent and comprehensive legal requirements in the context of addressing the crime of cyberstalking, even though previous laws and policies set significant precedents for cybersecurity and IT in Pakistan.

This law addresses the problem of cyber harassment that plagues contemporary culture and provides instant legal safeguards to the victims. Thus, the void that was provided by prior laws is filled. According to an analysis of the PECA, Section 24 clause on cyberstalking, victim rehabilitation or mental health assistance must be offered. The government ought to set up rehabilitation facilities where individuals can get the facilities and mental health care they require. Complaints, the background of the cyberstalker, the technique for developing the victim-stalker relationship, and the therapy of any psychological trait may help to cease cyberstalking. However, cyberstalking cannot be stopped by sanctions and complaints alone (Lapshin & Klimakov, 2019).

## Overview of Cyberstalking Laws in the United States

One of the first countries to enact federal and state laws against cybercrime was the United States of America (Moise, 2017). According to The Interstate Communications Act of 2012, anyone who sends a communication across state or international lines with the intent to extort, including threats to harm someone or their property, damage their reputation, or commit kidnapping, faces a fine, up to two years in prison, or both. This law is one of two important federal laws that address cyber harassment, including cyberbullying and cyberstalking. The Interstate Stalking and Prevention Act of 1996, specifies various jail sentences for those who use electronic

communication devices to cause mental distress or to instill a reasonable fear of death or serious damage in another person (United States Department of Justice, 2016). There are various ways to deal with cyberstalking under federal law. The Interstate Communications Act of 2012 states that sending any message over state or international borders that contains a threat to injure someone is a federal offense, punishable by up to five years in prison and fines of up to $250,000.This section covers any form of communication transmitted across these lines, including threats made via telephone, email, beepers, or the Internet. Certain types of cyberstalking can also be prosecuted under 47 U.S.C. § 223 of this Act. According to this law, using a phone or other telecommunications device to irritate, abuse, harass, or threaten someone at the dialed number is a federal offense that carries a maximum sentence of two years in jail, provided the offender keeps their identity a secret (The Interstate Communications Act of 2012).

This law only applies to direct communications between the offender and the victim, even though it covers both threats and harassment. It doesn't apply when someone uploads offensive content on message boards or in chat rooms to provoke others or to annoy or upset someone. Furthermore, breaking Section 223 carries a maximum sentence of two years in prison and is classified as a misdemeanor (US Department of Justice, 1999). Section 646.9 of the California Penal Code, which was passed in 1999, made California the first state in the United States to pass legislation against cyberstalking (Dean, 2000). It was initially used to sentence a man who harassed a woman who could identify him to six years in prison (Zeller, 2006).

A California legislation that went into effect on January 1, 2009, allows schools to suspend or expel pupils for harassing their friends online. It also mandates that schools have measures in place to address the problem (Calefati, 2009). Furthermore, Section 1708.7 of the California Civil Code outlines the grounds for bringing a general, special, and punitive damages lawsuit against one's cyberstalker and any collaborators. (Civil Code, 2011). Florida Statute 784.048 defines "cyberstalking" as a pattern of behavior that includes sending or causing to be sent words, images, or language via electronic mail or communication to a specific individual, causing significant emotional distress without any legitimate purpose. This is classified as a first-degree misdemeanor; if the victim is a child under 16 or if the offender has been legally ordered not to contact the person, the offense is classified as "aggravated stalking," which is a third-degree felony; additionally, cyberstalking combined with a credible threat is also considered aggravated stalking. In California, cyberstalking is covered by the California Civil Code, which allows victims to seek damages for harassment and stalking carried out through electronic means (The Florida Legislature, 2014). One of the first laws against cyberstalking was passed in Washington in 2004 and states that utilizing electronic communications to harass, intimidate, torture, or embarrass someone is illegal. Someone will be charged with a serious misdemeanor if they repeatedly harass someone, use profane or obscene language, or make bodily threats (Cyberstalking, 2022). The U.S. federal criminal code contains multiple sections that federal investigators and prosecutors use to deal with cyberstalking. Usually imposed federal offenses in recent cases connected to acts of stalking arise from the following sections: -

- 18 U.S.C. § 875(c): Making threats to hurt someone else

- 18 U.S.C. § 1952: Extortion, including sextortion, through interstate communications.

- 18 U.S.C. § 2251: Using various forms of compulsion or persuasion to engage a juvenile in child pornography.

- 18 U.S.C. § 2422(b): Luring or pressuring a juvenile into engaging in sexual behavior through interstate communication.

- 18 U.S.C. § 2425: luring a minor into engaging in illicit sexual activity through interstate or international trade, including over the phone and the internet.

- 34 U.S.C. § 12291(a) (8): committing violence against an intimate partner.

- 47 U.S.C. § 223: Deceiving, annoying, abusing, harassing, or threatening someone anonymously over the phone or through text message using a telecommunications device.

While these statutes may apply to various aspects of cyberstalking, they each address specific behaviors associated with cyberstalking, such as threatening, harassment, sexual coercion, hacking, and extortion, rather than defining cyberstalking as a distinct crime. These statutes were enacted between 1934 and 1998, with later amendments. (Blanch and Hsu, 2016)

**Overview of Cyberstalking Laws in the United Kingdom**

In Wales and England, cyberstalking was formally recognized as a criminal offense under the Protection of Freedoms Act of 2012. This law listed the essential components of cyberstalking, such as contacting someone, following them around in public or private areas, conducting online monitoring, interfering with someone else's property, or spying on them. Additionally, it added sections 2A and 4A to the Protection from Harassment Act of 1997, creating two new stalking offenses. Engaging in stalker behavior is illegal under Section 2A of the Act if:

(a) It amounts to harassment of the individual.

(b) The actions or inactions involved are associated with stalking, and

(c) The perpetrator knows or should have reasonable knowledge that their actions constitute harassment of the other person (Protection from Harassment Act (1997). The Act provides a non-exhaustive list of behaviors associated with stalkers, although it does not define stalking expressly. Examples of cyberstalking include keeping tabs on someone's usage of the internet, email, or other electronic communication channels in an effort to make any kind of contact with someone or disseminate information that is inaccurately ascribed to or about someone. This proves that cyberstalking is recognized as a subcategory of stalking under section 2A of the Act. A fine of up to level 5 on the standard scale, up to six months in prison, or both could be imposed on anyone found guilty under this clause. In relation to the section 2A offense, section 2B gives police further permission to enter and examine properties. More severe forms of stalking are covered by Section 4A, particularly those that include causing severe alarm or distress or inciting a fear of violence. A pattern of behavior constitutes a section 4A offense.

It is equivalent to stalking if it either causes the victim to become extremely alarmed or distressed, which severely disrupts their everyday life, or if it makes them worry that violence will be used against them at least two times. Because section 4A expands on the restrictions of section 2A, it is implied that it also includes more severe kinds of cyberstalking. If found guilty on indictment, a person convicted under section 4A faces up to five years in jail and/or a fine; if found guilty summarily, they face up to six months in prison and/or a fine up to the statutory maximum (Protection from Harassment Act, 1997). Section 39 of the Criminal Justice and Licensing (Scotland) Act 2010 made stalking a crime in Scotland. According to this section, someone is guilty of stalking if they engage in the course of behavior that is intended to cause fear or alarm, or if they knew or should have known that their actions would likely have such an effect. The victim must also have suffered physical or psychological harm or been afraid for their safety as a result of the behavior.

The Act's Section 31(6) lists a number of actions that fall under Section 39, such as cyberstalking, which includes publicizing remarks about an individual, contacting them by text, email, or other means, or monitoring their online or electronic communications activity. Given that this list is not all-inclusive, it can be deduced that this section also covers various types of cyberstalking. Due to the broad nature of the offense's mental component, which includes both subjective and objective elements, it can be proven that the accused should have known or intended for their actions to cause harm. The extent of the violation, however, can be constrained by the victim's bodily or psychological injuries (Criminal Justice and Licensing, Scotland Act 2010). Subsection (5) allows a person accused of violating this section to defend themselves by arguing that the conduct: "(a) was authorized by any law or enactment, (b) was carried out to prevent or detect crime, or (c) was reasonable in the specific circumstances."

However, since stalking is inherently unreasonable, using reasonableness as a defense seems to provide an unwarranted justification for such behavior. The Protection from Harassment (Northern Ireland) Order 1997, which is identical to the original, un-amended version of the Protection from Harassment Act 1997 applied in England and Wales prior to the 2012 reforms, largely addresses stalking. The Protection from Stalking Bill, which Northern Ireland presented to its Assembly in January 2021, has not yet been signed into law. In England and Wales, the bill's provisions align with section 2A of the Protection of Freedoms Act 2012; nonetheless, the measure does not need evidence of the victim's actual physical or psychological harm, in contrast to the UK Act(Munasinghe & Harasgama, 2002). Prior to the Online Safety Act (OSA) 2023's partial repeal, Section 127 of other acts pertaining to cyberstalking and cyberharassment specifically addressed harmful communications over public electronic networks. Cyberstalking can be addressed under this section if the stalker sends offensive, obscene, or menacing messages via social media, emails, or other electronic communications (Communication Act 2003). The partial repeal by OSA 2023 indicates that these practices will be increasingly regulated under newer online safety laws.

Section 1 of the Communications Act 1998 specifically addresses sending harmful messages to cause anguish or anxiety. Cyberstalking frequently entails sending repeated threatening or distressing messages, which would fall under this section (Communications Act 1988). Section 179 of OSA 2023 introduces more comprehensive online safety regulations,

addressing harmful online behaviors like cyberstalking. It imposes obligations on platforms to prevent the spread of harmful content, which includes cyberstalking activities like persistent harassment or stalking through social media or other online platforms (Online Safety Act, 2023). Section 181, OSA 2023, addresses the penalties for noncompliance by platforms that do not forbid cyberstalking. It also provides enforcement strategies for online safety law infractions, which may include cyberstalking (Online Safety Act, 2023).

**Comparative Analysis of Cyberstalking Laws of USA and UK with Pakistan**

Comparative cyberstalking laws in the USA, Pakistan, and the UK show similarities and variations in these disparate responses to online harassment and threats. An inclusive paradigm for cyberstalking has been created in the United Kingdom. The Protection from Harassment Act of 1997 is amended by the Freedoms Act of 2012 to add particular measures about stalking, including cyberstalking. Conduct that qualifies as harassment is illegal under Section 2A, including frequent contact and internet surveillance. This offense carries a maximum six-month jail sentence as well as a fine. Section 4A addresses more severe situations when there is a significant risk of violence or significant anguish and stipulates punishments of up to five years in jail.

The UK's viewpoint extends to the recent 35 advancements in online safety through the Online Safety Act 2023, which sets a duty on platforms for the control of hazardous content, including cyberstalking.

In the USA, federal statutes handle such items as 18 U.S.C. § 875(c) and 47 U.S.C. § 223 deal.

With threats, harassment, and cyberstalking that are transmitted across state lines or under a false identity. Significant penalties, including up to five years in prison, are permitted under federal law in addition to hefty fines. Certain statutes apply to other connected offenses, such as sextortion and the online enticing of minors. This covers general threats in a broad sense, while the US approach has laws that address specific types of cyberstalking.

Pakistan's cyberstalking laws are less comprehensive than those in the United Kingdom and the United States. The Prevention of Electronic Crimes Act of 2016 is the main piece of legislation that addresses online harassment. PECA makes a variety of cybercrimes illegal, including

Cyberstalking is defined as the use of electronic methods to harass or threaten an individual. This law stipulates that among other punishments, the accused may be found guilty and subject to fines and imprisonment. PECA includes provisions addressing a number of cybercrime-related issues, including data breaches and unauthorized access to information. However, in comparison to the UK and the USA, PECA is less thorough in its legal framework regarding cyberstalking.

The Pakistani approach under PECA covers cyberstalking from a broader perspective of electronic crimes, while the United Kingdom and the United States have enacted specific laws that specifically target cyberstalking and its variants, with recent updates and comprehensive coverage of the subject matter. The UK law developed a sort of subtle understanding of the concept of cyberstalking by framing it as a general and aggravated offense and providing a detailed penalty, with recent updates aimed at online safety. As a result, the US legal system contains federal statutes related to the various aspects of cyberstalking, with sentences relating to threats and harassment being the harshest.

In Pakistan, it provides a basic framework, but lacks the precision and detail present in the UK and USA, thus necessitating future development to reach a more extended standard in the elements associated with cyberstalking.

## RECOMMENDATIONS

Pakistan's cyber laws must be aligned with international norms and best practices. The general public is becoming more and more engrossed in the digital world as social media usage and computer dependence increase. Every bachelor's and master's degree program should include cyber law and cybercrime courses to address this and raise public awareness, especially concerning cyberstalking and cyber harassment.

The general public should have access to a guidebook that accurately describes cyber laws and cybercrimes, and educational programs should be updated to reflect contemporary demands. Additionally, a comprehensive study is necessary to ascertain the actual effects of cybercrimes, including cyberstalking and cyberharassment, on a range of industries, including the economy, people of all ages, banks, governmental institutions, and the broader technical industry.

The PECA, 2016 act needs to be updated to clearly describe the various types of cyberstalking, much like the Protection from Harassment Act in the UK and federal laws in the USA do. As a result, different types of cyberstalking would be classified into distinct categories, and suitable punishments would be prescribed, eliminating any coverage gaps.

Pakistan's police and judges will benefit greatly from specialized training programs that will help them comprehend a variety of difficulties pertaining to the implementation of cyberstalking legislation. Similarly, when it comes to identifying, looking into, and punishing cyberstalking, Pakistani authorities ought to follow some implementation tactics from the United Kingdom and the United States.

Establishing cybercrime sections for law enforcement organizations that are at least sufficiently prepared with the necessary equipment and expertise to handle only cyberstalking cases would be more effective and efficient. These might involve international cooperation with nations such as the United Kingdom and the United States that have adopted best practices.

## REFERENCES

Blanch, J. L., & Hsu, W. L. (2016). An introduction to violent crime on the Internet. *United States Attorneys Bulletin, 64*(3), 1-12.

Bocij, P. (2004). *Cyberstalking: Harassment in the Internet age and how to protect your family.* Praeger Publishers. Retrieved from https://dl.acm.org/doi/abs/10.5555/983807

Calefati, J. (2009, January 7). California law targets cyberbullying. *U.S. News.*

California Civil Code 1708-1725. (2011). *Wayback Machine.* Retrieved from https://web.archive.org/

Chik, W. (2008). Harassment through the digital medium: A cross-jurisdictional comparative analysis on the law on cyberstalking. *Journal of International Commercial Law and Technology, 3*(1), 18-28. Retrieved from https://www.researchgate.net/publication/26492206_Harassment_through_the_Digital_Medium_A_Cross-Jurisdictional_Comparative_Analysis_on_the_Law_on_Cyberstalking

Communications Act. (2003). *Section 27.*

Criminal Justice and Licensing (Scotland) Act. (2010). *Section 39(3) and 39(4).* Retrieved from https://www.legislation.gov.uk/asp/2010/13/section/39

Cruz, V. F., Agustina, J. R., & Ngo, F. T. (2021). An exploratory investigation of traditional stalking and cyberstalking victimization among university students in Spain and the United States: A comparative analysis. *IDP: Revista de Internet, Derecho y Política, 32*, 9.

Cyberstalking. (2022). *Chapter 9.61.260.* Wa.gov. Retrieved from https://app.leg.wa.gov/rcw/dispo.aspx?cite=9.61.260

Dean, K. (2000, May 1). The epidemic of cyberstalking. Retrieved from https://www.wired.com/2000/05/the-epidemic-of-cyberstalking/

Fisher, B. S., Cullen, F. T., & Turner, M. G. (2002). Being pursued: Stalking victimization in a national study of college women. *Criminology & Public Policy, 1*(2), 257-308. Retrieved from https://onlinelibrary.wiley.com

Haq, I. U., & Zarkoon, S. M. (2023). Cyberstalking: A critical analysis of the Prevention of Electronic Crimes Act-2016 and its effectiveness in combating cybercrimes: A perspective from Pakistan. *Pakistan's Multidisciplinary Journal for Arts & Science*, 43-62.

Lapshin, I. Y., & Klimakov, A. V. (2019, July). Cyberbullying and cyberstalking as a moral and legal concept. In *4th International Conference on Contemporary Education, Social Sciences, and Humanities (ACCESS 2019)* (pp. 1857–1861). Atlantis Press.

Maple, C., Short, E., Brown, A., Bryden, C., & Salter, M. (2012). Cyberstalking in the UK: Analysis and recommendations. *International Journal of Distributed Systems and Technologies (IJDST, 3)* (4), 34-51.

Moise, A. C. (2017). The legal regulation of cybercrime in the United States of America legislation. *Journal of Advanced Research in Law and Economics (JARLE, 8 )*(27), 1576-1578.

Munasinghe, P., & Harasgama, K. (2021). A comparative analysis of cyberstalking legislations in the UK, Singapore, and Sri Lanka. *SSRN Electronic Journal*. Retrieved from https://dx.doi.org/10.2139/ssrn.3903800

Online Safety Act. (2023). *Section 179.*

Online Safety Act. (2023). *Section 181.*

Pakistan Electronic Crimes Act. (2016). *Section 24.*

Protection from Harassment Act. (1997). *Section 2A.* Retrieved from https://www.legislation.gov.uk/ukpga/1997/40/contents

Protection from Harassment Act. (1997). *Section 4A.* Retrieved from https://www.legislation.gov.uk/ukpga/1997/40/contents

Shambhavee, H. M. (2019). Cyberstalking: Threat to people or bane to technology. *International Journal of Trend in Scientific Research and Development (IJTSRD, 3)*(2), 350-355.

Spitzberg, B. H., & Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. *New Media & Society, 4*(1), 71-92. Retrieved from https://journals.sagepub.com/doi/abs/10.1177/14614440222226271

Stalking Protection Act. (2019). *UK Government.*

The Florida Legislature. (2014). *The 2014 Florida Statutes.* Retrieved from https://www.leg.state.fl.us/statutes

The Interstate Communications Act. (2012). *18 U.S.C. § 875.* Retrieved from https://uscode.house.gov

The Interstate Communications Act. (2012). *47 U.S.C. § 223(a) (1) (C).* Retrieved from https://www.law.cornell.edu/uscode/text/47/223

United States Department of Justice, Executive Office for United States Attorneys. (2016). Cyber misbehavior. *Washington, DC: United States Department of Justice.*

US Department of Justice. (1999). Cyberstalking: A new challenge for law enforcement and industry: A report from the Attorney General to the Vice President. *Office of Justice Programs.* Retrieved from https://www.ojp.gov/ncjrs/virtual-library/abstracts/cyberstalking-new-challenge-law-enforcement-and-industry-report

Zeller, T. (2006, April 17). Despite laws, stalkers roam on the internet. *The New York Times.*