PMDJAS
E-ISSN: 2789-2611
Pakistan's Multidisciplinary Journal for Arts & Science
ISSN 2789-2611
https://pmdjas.com
| December. 2023, VOL. 4 (No, 03) Page. 43 – 62 |

Cyber Stalking: A Critical Analysis of Prevention of Electronic Crimes Act-2016 and Its Effectiveness in Combating Cyber Crimes, A Perspective from Pakistan

Ihtaram Ul Haq[1], Shah Muhammad Zarkoon[1]*

[1]University Law College, University of Balochistan, Quetta, Pakistan

DOI: https://doi.org/10.5281/zenodo.10450177

Corresponding Author, Shah Muhammad Zarkoon: smzarkoon@gmail.com

Received December: 08/2023. Accepted December: 26/2023. **Published December: 30/2023.**

Abstract

The number of cybercrimes in Pakistan is growing rapidly. The study analyzed and described cybercrimes and all the elements that contribute to them. It covered all the common methods by which cyber criminals commit crimes. This study discusses how cyber stalking is a great threat to the world. Cyber stalking means to "stalk or harass" an individual, organization, or organization over the internet or other forms of electronic communication. More broadly, cyber stalking includes defamation, discrimination, demeaning others, and baseless allegations. Stalking has been recognized as a major problem in both academia and the media since the late 1980s and early 90s. The Federal Investigation Agency's (FIA) approach to cybercrime investigation in Pakistan is examined and assessed in this paper. The goal of this study is to give a thorough look at cybercrime in Pakistan and to question whether the new law, the Prevention of Electronic Crimes Act 2016, was adequate to fight cyber criminals, cyber stalking, and other related issues. What other rules and restrictions can be put in place to further regulate internet users and prevent cybercrime?

Keywords: Cybercrime, Cyber stalking, Protection of Electronic Crimes Act, 2016

INTRODUCTION

In this technologically advanced era, the whole world has formally stepped into the digital world. Everyday tasks are becoming easier as a result of technological advancements. Having said that, they do play a major role in criminal activity. The rapid development of current technology makes cyber stalking a greater threat (Horgan 2019). To "stalk" or "harass" an individual, organization, or organization over the internet or other forms of electronic communication is cyber stalking. More broadly, cyber stalking includes defamation, discrimination, demeaning others, and baseless allegations (Chawki et al.,2015).

In today's world, stalking is a major problem. As more and more people identify themselves online, a new kind of stalking known as cyber stalking has emerged with the increasing popularity of social media (Woodlock 2017). The Internet has turned into a virtual haven for a brand-new, distinctive kind of criminal known as the "cyber stalker" (DeNardis L.2017).Stalking includes several methods, including tracking an individual to their residence or place of work, making unwelcome sexual approaches, harassing someone online, threatening physical harm, engaging in identity fraud, vandalizing their property, sending written messages or things, or engaging in repeated and bothersome phone calls (Ghosh 2021). The Internet makes it easy to breach someone's privacy while staying anonymous. As people share more and more information online, distinguishing between what is public and what is private becomes increasingly difficult. The current environment has changed expectations of privacy, including its definition, scope, and level. Privacy expectations have changed communication and increased chances to monitor, harass, and pursue others (Dakota 2015).

BACKGROUND

Stalking has been recognized as a major problem in both academia and the media since the late 1980s and early 90s (Moriarty 2008). The state of California successfully prosecuted the first case of cyber stalking on April 28, 1999, in accordance with a new Penal Code created as a result of the Violence Against Women and Department of Justice Reauthorization Act (Smith 2018). As a method of stalking, the Act includes "electronic" messages as an offense. After pleading guilty to "one count of stalking and a total of three charges of solicitation of sexual assault" against a lady who was 28 years old, Gary S. Dellapenta, a former security guard who was 50 years old, faced the possibility of serving up to six years in prison. The victim didn't have a computer and had rejected Dellapenta romantically after meeting him at church. Dellapenta impersonated her on the Internet, posting on message boards and chat rooms about her thoughts of being raped. He also shared her contact details on the internet, including her home location and phone number, which led to at least six odd males knocking on her house, claiming they wanted to rape her (Regehr at el.,2010).

Over the past twenty years, the Internet has grown at a rapid pace, ranking among the fastest-growing technologies ever created. In 2000, there were around 361 million Internet users worldwide. Currently, there are roughly 4.574 billion users around the globe. The number of victims of cyber stalking has also increased, with the U.S. Department of Justice claiming that over 1.3 million people fall victim to this kind of harassment each year. Between November 2022 and January 2023, a worldwide poll revealed that 36% of the respondents confessed to stalking a former or present partner using one of the previously mentioned methods. A total of 14% of individuals looked over their partner's phone in order to view images, phone calls, text messages, social media accounts and messages, or e-mails (Statista 2023).

Data Report says that in January 2021, 61.34 million people in Pakistan used the internet. Between 2022 and 2023, the number of Internet users in Pakistan rose 5.4%. As of January 2023, the number of internet users reached 87.35 million (Kemp s. Digital 2023). Since more people are using the internet, more bad things are happening online, which is what cybercrime is all about. Pakistanis, on the other hand, don't pay much attention to things like cybercrime. They're mostly busy with routine tasks. Most of the time, they don't know what tools cybercriminals use. The least that Pakistan can do to help with cyber security is almost nothing. Other groups, like the FIA, are doing their best to handle things, but things are getting worse (Akhlaq 2021). The main reason why cybercrime laws are not being enforced to the extent that they should be is the general public's lack of awareness and literacy. Another common problem is that people often do not realize their actions actually violate cybercrime laws. The public and the FIA, as the governing body on cybercrime, must work together to close the information gap, increase the number of reported crimes, and ensure the effective and efficient execution of the law (Akhlaq 2021).

CYBER LAWS IN PAKISTAN

Cyber laws, often known as online regulation, include the official concerns related to the distribution, communication, and transactional aspects of networked gadgets and technology. The President of Pakistan adopted the "Prevention of Electronic Crimes Ordinance" in 2007 with the intention of establishing legal protections against crimes committed online. But this was modified by the Prevention of Electronic Crime Act (PECA) of 2016 and is currently the law that Pakistan uses to punish cybercrimes. Different types of cyber offences that can be carried out using the internet and computer systems have been established in PECA 2016 which includes.

a) Cyber stalking

b) Hate speech.

c) Cyber terrorism

d) Incidents involving minors and human beings that violate their modesty.

e) Spoofing

f) Spamming

g) Tampering with data or information systems vital to the infrastructure

h) Electronic forgery

i) Altering communication devices

j) Terrorist recruiting, financing, and planning.

k) Data theft (including unauthorized copies or transmissions)

l) Child pornography

m) Glorification of an offense

n) Electronic fraud

o) Unauthorized duplication or dissemination of vital infrastructure data

p) The issue of a SIM card without authorization

q) Data loss (unauthorized access to vital infrastructure)

r) Violations of another person's dignity

s) Tampering with data or an information system

t) Gaining unauthorized access to data or an information system

u) The misuse of personal identification data

RECOGNIZED CYBERCRIMES COMMON IN PAKISTAN

Following are some common types of cybercrime that are well recognized:

Cyber Defamation

Cyber defamation refers to the act of spreading lies about a person or company via the internet or other digital communication channels, including social media, emails, instant messaging, or any other similar platform. Spreading lies about a person or company in order to damage their reputation is known as defamation. False charges, harmful rumors, or unfounded claims about someone posted on social media or another online platform are all examples of cyber defamation. For these cases of cyber bullying, the relevant sections of the Penal Enforcement Act of 2016 (PECA, 2016) are 20 and 21, which address violations of human dignity (Khan et al.,2023)

Identity Theft

The act of acquiring another person's financial or personal information with the intent to conduct fraud, such as making unlawful purchases or transactions, is known as identity theft. Identity theft may take many forms, and the victims usually suffer consequences for their reputation, wealth, and credit. For example, criminals use several methods to steal credit card information from company databases and then lower the victim's credit score. There are many different types of identity theft, but some of the most common include medical, financial, social security, tax, and driver's license fraud, as well as criminal identity theft (which involves using a victim's fake ID or other verification documents) (Hedyayati 2012).

Internet Fraud

The term "internet financial fraud" describes any kind of fraud scheme that makes use of email, social media apps, message boards, chat rooms, and other online platforms to conduct fraudulent transactions, pose as potential victims, or transfer the proceeds of the scheme to other participants or financial institutions. Social media is the simplest method to communicate with people and obtain their personal information, which is why con artists utilize it to trick individuals all over the world (Akram and Kumar 2017).

Online Harassment

When someone or a group consistently utilizes social media and information resources to damage or injure another, it is known as online harassment. This may involve exposing, demeaning, or threatening someone online. Sexual abuse based on images, online sexual harassment, and cyber stalking. It takes place on social media platforms including Facebook, Instagram, Snapchat, TikTok, and Twitter, as well as via email, SMS, and instant messaging (Bojilov 2023).

Cyber Terrorism

Terrorist groups now have a new playground in which to pursue their objectives by staging attacks or threats against computer networks and information systems as a result of the expansion and increase in social, political, and economic dependency on the internet. A lot of countries, like the UK and the US, have passed different rules to stop this. Many experts have given it different definitions based on their own points of view. Verton described it as "an unexpected attack on a country's physical and electronic infrastructures by a sub national foreign terrorist group or individuals with a political agenda in their own country using computers and the Internet to destroy or disable them"(Usman M 2017).

Political Hatred

Activists from different political parties have set up social media groups to help their parties reach their goals. Their only goal is to back the plans of their own party and criticize the plans of their opponents. Several cases have been brought against politicians due to the spread of political hate through these kinds of actions on social media. Because of this, political talk has become more vicious and unacceptable. Because of these events, political anger has grown across the country (Ernst et al.,2017).

Religious Hatred

People can also find blasphemous and hateful material promoting religion on social media. There are a lot of websites where people may post videos and articles that are critical of other religions and groups. Some people find this content offensive. A few political and religious groups, for example, used their statements and the internet to stir up violence at their sit-ins in Faizabad, which violated the rights of the public. Bad things happened to people's cars and other things they owned. Also, a few people died. Road closures made it difficult for people to move around easily (Venkiteswaran 2017).

Cyber Stalking

In today's world, stalking is a major problem. As more and more people identify themselves online, a new kind of stalking known as cyber stalking has emerged with the increasing popularity of social media. Cyber stalking is also addressed under Section 24 of the PECA-2016.

CYBERCRIMES CENTERS IN PAKISTAN

The Pakistani government set up the "National Response Centre for Cybercrime (NR3C)" under the administrative control of the Federal Investigation Agency (FIA) to investigate cybercrimes. The FIA has set up fifteen anti-cybercrime centers. These centers have "expertise in digital forensics, technological investigation, audits of information systems security, penetration testing, and training." Yet, there are so many centers around the nation that each one must handle complaints from many districts. As an example, the cybercrime center in Lahore is responsible for investigating all reported cases in the Lahore and Sahiwal divisions, a total of seven districts with a population of around 27 million people (Agency fi. National response center for cybercrime 2021).

Despite the formation of cybercrime centers and even an online way to file complaints, reports of cybercrime aren't common, and bank and credit fraud are among the least common types of reported cybercrime. Cyber bullying, cyber stalking, and defamation are the most common types of cybercrime. The new laws made under PECA are not well known among most people in Pakistan. The process of filing a police report (FIR) on the grounds of cyber bullying is still relatively new and is often seen as an unnecessary burden, leading many victims to choose to ignore such trivial crimes, resulting in no legal consequences. Cybercrime is still one of the least reported crimes in Pakistan and is also perhaps one of the most ignored and committed crimes in the country. This is mostly due to the public's lack of awareness and desire to take action (Express TT. Only 14 cybercrime convictions in five years. 2020).

THE ACT OF REPORTING A CYBERCRIME

Complaints about cybercrime may be sent online via the National Reporting Center (NR3C) website, which can be accessed at www.nr3c.gov.pk. The complainant must include their name, family history, gender, telephone number, personal identification number, email address, and information about the offense. Additionally, the victims have the option of going to the regional NR3C offices. Crimes such as unauthorized access to electronic data or identity, hacking of email accounts or the creation of fake user IDs, online scams and frauds of a financial nature, and defamation on cyber media are those that are considered by NR3C (Munir and Gondal 2017).

OBJECTIVES OF THE STUDY

- The main objective of the study is to critically analyze whether the introduction of a new statute in the shape of the Prevention of Electronic Crimes Act 2016 met the requirements of the present era in order to combat the violators of cybercrimes and those who are involved in cyber stalking, etc., and what are the limitations and expectations that can be further imposed in order to control the netizens from cybercrimes and cyber stalking.

RESEARCH QUESTIONS

- Whether the Prevention of Electronic Crime Act 2016 (PECA) has been effective in combating cybercrimes and cyber stalking or not?

RESEARCH METHODOLOGY

The following sentences represent the approach that was used in this research.

RESEARCH DESIGN

The current research is qualitative and doctrinal library-based, which means it uses words and sentences instead of numbers. This research aims to analyze the legal concept by analyzing its origins, development, and implementation(24). This study was entirely theoretical and included either a simple inquiry seeking a particular declaration of the law or in-depth legal analysis using complex reasoning. In simple terms, it was a study conducted in libraries with the intention of obtaining the "one right answer" to specific topics or concerns related to law. Specifically, cyber stalking laws and PECA 2016 were the subject of an investigation. The key characteristics of doctrinal or library-based research are the provision of simple, verifiable solutions to all relevant problems. Among these procedures is the study of legal problems to see whether further research is necessary. This phase frequently involves considerable background reading on the topic matter from sources including dictionaries, encyclopedias, significant textbooks, treatises, and periodicals with footnotes. These resources provide definitions of terms to help in the student's understanding and summarization of the legal concepts related to the area of law being studied. This contribution's selected source list included national and international search papers, legislation, and policy studies that were released under legitimate research projects that covered the topic (Ali et al.,2017).

DATA COLLECTION

It includes research on international law as well as other subjects done in libraries. Electronic data includes an extensive selection of resources, such as books, manuals, journal articles, and more. Primary sources of information include books, periodicals, abstract directories, research papers, conference proceedings, market analyses, and reports. The secondary data source is built upon the foundation of these original sources: records of organizations that search for items in newspapers, magnet magazines, and other publications on the internet. It enables the successful collection and presentation of data.

PECA 2016: Precautions that Deal with Cybercrime and Stalking

Governments are working hard to improve the privacy of their citizens and regions (Demeties DS 2020). The Personal Electronic Communications Act (PECA) is a piece of legislation that aims to protect individuals' rights and privacy while also establishing legal mechanisms for investigating and punishing offenses related to electronic and online activities (Aleem et al.,2021). The Electronic Transactions Ordinance (ETO) had already made it illegal in Pakistan to unlawfully access information without authorization before the passage of the Prevention of Electronic Crimes Act (PECA) in 2016 (Aleem et al.,2021). Despite widespread disapproval from concerned human rights advocates and politicians, the PECA was implemented in August 2016 (Akhtar 2023). The implementation of this contentious legislation concluded a protracted and tense conflict between the government and the several parties involved, who criticized it as "a contradictory combination of measures that restrict freedom of expression, privacy, and online activities." In a nation such as Pakistan, where digital literacy is relatively poor, it would have been prudent to have formulated and implemented a well-crafted law addressing cybercrimes earlier. This law should have been executed with the necessary expertise and understanding to assure its compliance with the constitutional framework (Jamshed et al.,2022).

a) **Illegal Access of Data:** A person who obtains unauthorized access to a data system or information system with the aim to commit dishonesty is liable to a jail sentence of up to three months or a penalty of up to 50,000 rupees, or both, depending on the severity of the conduct.

b) **Illegal Transmission of Data:** A fine of up to 100,000 rupees, six months in jail, or both may be imposed on anybody found guilty of illegally duplicating or transmitting data without the necessary permission.

c) **Interfering With Data:** An offender faces a maximum of two years in jail and/or a fine of 500,000 rupees (or both) for willfully interfering with, damaging, or causing interference with any portion or whole of an information system/data.

d) **Illegal Access to Critical Organizational Data**: Someone might face up to three years in prison or a fine of one million PKR, or both, if they intentionally gain unauthorized access to data or systems related to crucial infrastructure.

e) **Illegal Replication of Crucial Infrastructural Data**: Individuals who intentionally and without authorization copy or transmit material related to important infrastructure with the goal of deceiving others are accountable to a maximum sentence of five years in jail. Another possibility is that the punishment will consist of either a fine of up to five million rupees or both of these conditions.

f) **Interfering with Crucial Infrastructural Data:** A maximum of seven years in jail or ten million rupees in fines, or both, awaits anybody found guilty of intentionally interfering with or damaging a vital information system or any element of it.

g) **Glorification**: An individual commits a terrorism-related crime if they intentionally generate or distribute information using any form of technology or method. Anyone convicted of a crime involving terrorism or association with illegal groups or people faces a maximum penalty of ten million rupees fine or seven years in jail, or both. When anything is praised or celebrated in a positive manner, it is said to be glorified.

h) **Cyber Terrorism:** Anyone who commits or threatens to commit any of the crimes listed in sections d, e, f, or g with the goal of causing a widespread panic through the use of modern technological devices and computer systems is being charged with cyber terrorism. This includes hacking, information theft, and cyber-attacks (Jamshed et al.,2022). A person faces up to fourteen years in prison and a fine of up to fifty million rupees (or both) if they are found guilty of bribing, intimidating, creating anxiety, worry, or fear in the governing body, the general population, a particular group of people, a community, or a religious group; encouraging the spread of multicultural, tribal, or ethnic rivalry; or advancing the goals of organizations or groups forbidden under the law.

i) **Electronic Forgery:** To start with, anybody who manipulates information, networks, or devices in order to do damage to other people or the public at large is guilty of cybercrime. One possible penalty is a fine of two hundred and fifty thousand rupees, while another is a certain sort of imprisonment for a period of up to three years. If you want to trick someone into giving up their property or signing an agreement, you can use fraudulent claims, fake names, or data manipulation to make it look like the real thing, regardless of how easy it is to understand. Criminal penalties for violations of the first point of subsection include fines of up to five million rupees, imprisonment of up to seven years, or both.

j) **Electronic Fraud:** An offender faces a maximum of ten million rupees in fines or two years in prison if found guilty of intentionally interfering with or using any kind of technology, device, or data; convincing another person to get into a relationship; or deceiving any individual in a way that could cause harm or damage to themselves or others.

k) **Making, Obtaining, or Supplying Device for Use in Offence:** Anyone found guilty of creating, producing, buying, selling, presenting to supply, or importing any data, system, or device with the intent to commit or help in the commission of an offense under this Act could face up to six months in prison, a fine of up to 50,000 rupees, or both. This punishment applies regardless of any additional responsibility that person may face in the matter.

l) **Unauthorized Use of Identity Information:** A punishment of up to five million rupees, three years in jail, or both may be imposed on anybody found guilty of buying, trading, carrying, transferring, or using another person's identity without their consent. This is applicable to everyone whose personal data has been compromised. In order to protect, delete, restrict access to, or stop the transmission of identification information, one may contact the Authority. The Authority will promptly respond to such a request and take the necessary steps to protect, delete, or block the transfer of the requested personal information.

m) **Unauthorized Issuance of SIM Cards etc.:** To whom it may concern: those involved in the sale or provision of Subscriber Identity Module cards, reusable Identification Modules, universal integrated circuit cards, or any other module intended for user authentication in order to establish a network connection and to be utilized in cellular phones, wireless phones, or other electronic gadgets like tablets. Failure to gather and verify the customer's background information in accordance with the authority's current authorization could result in a fine of up to five hundred thousand rupees (or three years in Jail), or both.

n) **Tampering, etc. of Communication Equipment:** Those who change things in an unlawful or unauthentic way. The penalty for those who modify, tamper with, or reprogram the unique device identification of communication equipment, such as a cellular or wireless phone, and then use or sell such a device for sending and receiving information is imprisonment. Three years in jail, a fine of as much as one million rupees, or both might be the penalty.

o) **Unauthorized Interception:** Punishment is in store for anybody who knowingly and intentionally uses technological tools to intercept transmissions-whether they be inside a computer system or data sent by electromagnetic emissions-that are not intended for or accessible to the public. Two years in jail, a fine of up to 500,000 rupees, or both might be the terms of the sentence.

p) **Offences against the Dignity of an Individual:** A person can face up to three years in prison or a fine of up to one million rupees, or both, if they deliberately and intentionally transmit false information through any information system with the intent to deceive or harm the reputation or privacy of another person. This sub-section shall not apply to any media or distribution service covered by the Pakistan Electronic Media Regulatory Authority Ordinance, 2002 (XIII of 2002) with regard to any transmitted or distributed material.

q) **Offences against Modesty of a Natural Person and Minor:** The offender faces a maximum of five years in prison and a fine of up to one million rupees, or both, for the purpose of publicly showing or transmitting anything that applies a person's face on top of a pornographic video or picture. It contains a picture or video of someone engaging in inappropriate sexual behavior. Harassment is the use of sexually explicit language, images, or videos that incite hate, blackmail, damage a person's reputation, or seek retribution by encouraging or persuading someone to participate in a sexually graphic activity using an information system. Anyone found guilty of a violation under this provision involving a minor faces a maximum fine of five million rupees and a maximum jail sentence of seven years. A person must be fined and sentenced to 10 years in prison if they have a prior conviction for a violation under the aforementioned subsection involving a juvenile.

➢ **Child Pornography.-** Any person who intentionally makes, offers, offers access to, distributes, or transmits content through an information system, or obtains material in an information system for themselves or another person without lawful justification, faces a fine of up to five million rupees, seven years in prison, or both; (a) a minor engaging in inappropriate sexual behavior; (b) a person who looks to be underage associated with sexually explicit behavior; (c) realistic depictions of a minor engaging in sexually explicit behavior; or (d) the disclosure of the minor's identity. Anyone who feels harmed, or a minor's legal guardian may approach the authority to have the data mentioned in the previous section removed, destroyed, or restricted from access. As soon as the authority receives such a request, it will swiftly issue the necessary instructions, considering all relevant factors. Removal, destruction, transmission prohibition, or access-restricting orders are all examples of what can fall under this category. Also, the Authority can direct any of its licensees to keep such data, including traffic statistics, secure.

r) **Malicious Code:** There is a two-year jail sentence or a one-million rupee fine for anyone who, intentionally and without authorization, makes, gives, distributes, or transfers malicious code through an information system or device with the goal of damaging any information system or data and causing its tampering, theft, destruction, modification, suppression, fraud, or damage.

s) **Cyber Stalking:** A person commits cyber stalking when they intentionally use a computer, phone, email, or other electronic communication device to harass, threaten, intimidate, or force another person. The offender may be fined up to one million rupees, jailed for a term that might exceed three years, or both for the crime described in the previous section. The penalty for cyber stalking may be as severe as five years in jail or as high as 10 million rupees in fines, or both, in cases where the victim is a juvenile. Anyone who believes they have been harmed, or a minor's legal guardian, may ask for the data to be erased, blocked, or removed. The authority will immediately make suitable orders in response to such a request, taking into account what is acceptable under the circumstances.

t) **Spamming:** Defamation is the intentional transfer of unlawful, damaging, fraudulent, misleading, or unsolicited data to another person without their permission. Making use of any information technology to display such material dishonestly for personal gain is also included. People engaging in direct marketing, whether they be individuals, businesses, or organizations, have a responsibility to provide recipients with the option to stop receiving marketing messages. In the event that a person is found guilty of the crime of spamming, which involves the transmission of material that is damaging, deceptive, misleading, or unlawful; they will be liable to imprisonment for a term of up to three months, a fine of fifty thousand rupees, which may be escalated to five million rupees, or both of these penalties. Sending unsolicited material (often known as "spam") or engaging in direct marketing without permission is punishable by a fine of up to 50,000 rupees for first offenses. In the event that the offender commits another breach, they will be subject to a fine of at least fifty thousand rupees, with the possibility of reaching a maximum of one million rupees.

Spoofing: Anyone who creates a website on purpose or disseminates content from a fraudulent source with the intention of deceiving the recipient or visitor into believing that the information is accurate is engaging in spoofing. A punishment of up to 500,000 rupees (or three years in jail) or both may be imposed on anybody found guilty of spooling (Arshad 2018).

LITERATURE REVIEW

While conducting the literature review, the researcher looked at a large number of publications, including books, blogs, and theses. The researcher found significant differences between their study issue and the work conducted in the 21st century. The use of computers, smart phones, and other modern technology has grown in popularity. Cyber and, therefore, cybercrime became more common due to the increasing availability of modern technology and the prevalence of Internet-related difficulties and challenges in people's daily lives. Cyberspace is a result of the information technology revolution, where users of the Internet have equal access to data storage, information, and other resources. People are abusing modern technology more and more in cyberspace, which has caused a huge rise in Internet use. This has led to new cyber ideas like cyber stalking between people in different countries.

Asia is home to over 55% of the global population and has seen an enormous increase in the popularity and usage of web-based technologies over the past decade. Statista, a firm that specializes in the management of business process data, found that mobile phone devices accounted for 48.2% of the total internet traffic generated worldwide in November 2018. Consumers downloaded an additional 178.1 billion mobile applications from their mobile phone devices. In addition, technological convergence plays a significant part in our lives. In this context, the three C's, which are computers, content, and communication, are the primary pillars that support technology convergence (Singh 2019).

A recent study looked into studies to determine factors linked to both victims and perpetration of cyber stalking. Bitna Kim, a criminal justice professor at Sam Houston State University (SHSU), found approximately sixty papers on cyber stalking carried out between 2002 and 2022 as part of her research. Constantly threatening electronic messages were the focus of all the research. The United States accounted for 76% of the research, with other studies carried out in Turkey, Canada, Chile, Egypt, England, and Portugal. Both adults and teenagers were involved. Kim determined the relative importance of every factor associated with cyber stalking, including demographics (age, gender, sexual orientation, race/ethnicity), history (both online and offline), vulnerability (antisocial tendencies, attachment problems, family history of cybercrime), and protective factors (guardianship, security, protective traits, etc.). The end objective of her research was to identify any protective or risk factors associated with cyber stalking. Background had the greatest influence on cyber stalking criminal activity and victimization, followed by risk. Socio demographic and protective domains had not had a significant impact. Those who act aggressively online run the danger of being the target of cyber stalking or other forms of online revenge. There was a strong correlation between cyber stalking victims and criminal history, whether it occurred online or offline. Traits associated with unsafe relationships (such as infidelity, romantic jealousy, or threats) and personality and mental health issues (such as stress, anxiety, or depression) were significantly associated with cyber stalking and cyber stalking victimization. According to Kim, while thinking about ways to stop violence, it's important to consider how perpetrators and victims interact, as well as how physical and online forms of violence might overlap. People who have been victims of cyber stalking, whether online or offline, are more likely to be the perpetrators or victims themselves; thus, it's important that preventative efforts take this into consideration (Kim 2022).

A research study was carried out by Pyke *et al*. (2021) with the purpose of investigating the elements that prevent users from determining the severity of a cyber-attack. According to the study, victims of high-risk assaults had higher levels of awareness and unpleasant feelings than those harmed by low-risk attacks. The study also discovered that, in contrast to their peers with limited expertise, those with high knowledge were able to correctly identify the attacks. Furthermore, the study indicated that consumers' situational trust is low in the face of cyber-attacks, but their emotional response is strong to reduce the risk they face (Pyke et al.,2021).

According to Halder and Jaishankar, a great deal of respect was shown to teachers in the past, and they were given a prominent position in the lives of their students. Today, students between the ages of 12 and 24 are using social media to harass, threaten, insult, and spread hate against their teachers. They are doing this in order to intimidate them. Because of their anger or because they want special treatment from their lecturers, many students are turning to social media to take advantage of their professors. The abusers express their anger and rage at the educators using harsh words while also appealing to the audience's sympathies. Most victims do not attempt to engage the authorities, and Internet firms often do not provide any support to victims either, thus the crime rate continues to rise (Halder and Jaishankar 2013).

Among the top five cybercrime crimes reported annually are cyber pornography and sending messages to engage in sex trade or online sex trading. "Relations for Compensation" was a common means of communication among the criminals who engaged in prostitution. In exchange for sexual favors, middle-aged males are buying lavish presents and extorting money from young ladies, especially students. The authorities in Taiwan apprehended a number of individuals for soliciting sexual favors online using false identities. From 1999 to 2004, the percentage of cybercriminals in Taiwan who operated independently rose from 44% to 87%. Males make up a disproportionate share of Taiwan's criminal population, and most of those offenders have completed senior high school. The majority of cybercrimes committed by undergraduate and graduate students include the dissemination of communications about sex trade (Lu et al.,2006).

Saini *et al.*, stated that exploring the actions of cybercriminals and the societal impacts of cybercrime may lead to solutions that address this disadvantage. Approaches to combating these crimes may be roughly grouped into three types: Cyber legislation, education, and policymaking are all things that fall under the umbrella of cyber law. Cybercrime management strategies are either not working at all or aren't working at all in a number of nations. New paradigms for regulating cyber assaults are required, and the current body of information is becoming harder to crack due to this lack of effort (Saini 2012).

Another study done by Alkhalil *et al.* (2021) indicates that hackers develop fake applications that closely resemble legal online microloan applications. Users mistakenly download these applications under the impression that they are genuine, and as a result, they unknowingly submit sensitive personal information. In order to deceive customers into divulging their personal and financial information, criminals employ phishing methods. These strategies involve sending phony messages, emails, or websites that look to be from genuine credit app providers. Another research shows that cybercriminals can use stolen identities to request loans through these sites, putting the victim in a difficult position due to the illegitimate debt. A study revealed that dishonest individuals use bogus information to request loans from many online microloan applications all at once, and they have no intention of paying them back. Criminals switch the victim's SIM card using weak identity verification procedures, granting them access to the victim's phone number and, eventually, their credit app accounts (Alkhalil 2021) (Gies SV et al.,2021)

Haider *et al.*, (2023) explained in their research about Muhammad Daniyal Farrukh Ansari vs. The State (2021), in which the accused faced multiple charges, including those relating to the complainant's dignity and modesty. The Supreme Court granted him bail, reasoning that the accused had not violated the prohibitory clause with the offenses he was accused of. It is clear from this case that the punishments that are outlined in various provisions of the PECA (2016) are insufficient when compared to the severity of the offenses. The victim and his or her family may suffer irreversible damage as a result of the serious crime of defamation, which is a serious offense.

The accused committed fraud on the complainant in the matter of Sheraz Khan vs. The State (2021) by using Facebook and WhatsApp linkages to defraud the complainant out of a total of Rs. 28,57,230/-. The Lahore High Court granted the accused person's request for bail. The Lahore High Court ruled that the accused cannot be tried together for offenses under the PECA and general laws, while releasing them on bond. Despite the evident inappropriate use of social media by the accused in the discussed case, they were still able to exploit flaws in PECA, 2016. The enforcement of other laws, such as the Pakistan Penal Code, 1860, the Criminal Procedure Code, 1898, and the Qanoon Shahadat Order, 1984, is allowed under Sections 28 and 44 of the legislation passed in 2016, as long as these laws do not contradict the specific provisions of the PECA, 2016. It is possible for the defendant to take advantage of a number of differences and loopholes in the PECA, 2016, as well as other basic fundamental and procedural criminal legislation, throughout the bail and trial stages. Further the researcher stated that the matter of Waheed Dhehphal Chandio v. The State (2019), in which, after getting a divorce, the accused revealed obscene recordings of his wife and sister-in-law that he had shot when they were engaged and married, respectively. The accused also used social media to send the girls' families recordings that were too sensitive. The authorities initiated his criminal prosecution under the provisions of the PECA, 2016 (articles 20, 21, and 24) (Haider et al.,2023).

The Electronic Transaction Ordinance 2002, according to Mehboob Busan's masterwork research paper "Cyber Crimes: A Case Study of Legislation in Pakistan in Light of Other Judges' Jurisdiction," does not sufficiently penalize cybercrimes. After Mehboob Busan suggested increasing the severity of these sanctions, the Pakistani government introduced new legislation in 2016 to address the issue. In Pakistan, one magistrate and one session handle issues related to cybercrime at the provincial level as part of the implementation of the legislation platform. It is also crucial to stay here because no research of this kind has been done before to determine that these courts are provided with contemporary technology and that the judges are trained to understand the fundamentals of cybercrimes. When technology is used to describe a crime, it is crucial to determine the average punishment, which is a quote specific to Pakistan.

CONCLUSION

This study analyzes cybercrime in Pakistan and the government's and law enforcement's countermeasures. Internet connections have exposed a large percentage of the population to cybercrime, and as technology advances, cybercrime keeps growing, forcing the government to act to protect its citizens. Being able to eliminate cybercrime is impossible since tens of thousands of new cybercrimes develop every day. Despite agency and legislative efforts, these incidents are hard to avoid. In Pakistan, which addresses enormous issues and economic problems, cybercrime, and punishment for it are not the government's top priorities. Therefore, a problem that is prevalent and vital to national security and population welfare is usually given minimal importance.

Online purchasing, banking, and marketing have undeniably made people's lives easier. But it has also put them at risk of cybercriminals who violate their privacy. Many businesses, both big and small, don't have the staff or training to properly secure sensitive information, leaving them vulnerable to privacy breaches and data theft. A wide variety of criminal activities, including white-collar crimes, violent crimes like terrorism and murder, and counterintelligence operations like spying, fraud, and drug trafficking, may be committed through the use of technology. Because of loopholes in its provisions, the Act is failing to accomplish its principal goal. In addition, the Act needs further provisions to make it more effective and easier for the courts to implement.

These shortcomings have faced significant criticism due to the Act's flawed drafting process. This paper focuses on the Pakistan Electronic Crimes Act of 2016, which defines a number of cybercrimes. For all practical purposes, cybercrime is serious and poses a danger to humans everywhere. People can protect their personal information from cybercriminals by using full-service network security, strong passwords, keeping their software up to date, teaching their kids about the internet, and being aware of what to do if they become a victim. Reading this article will give you a better understanding of cybercrime in Pakistan and what the government can do to stop it.

LIMITATIONS

The absence of information on incidents in Pakistan and the actions taken by the government in response to them was a major shortcoming of my research. Data from the court is difficult to get, and FIA does not let anyone research ongoing cases. Data on the internet is also limited.

RECOMMENDATION

Due to the nature of cybercrimes, which makes them extremely sensitive, the Federal Investigation Agency must follow these recommendations for an in-depth investigation.

- ➢ The investigative department should provide the tools required for looking into such offenses.
- ➢ Legislation related to cyber in Pakistan must adhere to standards and best practices established on a global scale. Every day, we rely more and more on computer systems, and the rise of social media has done nothing but entice the entire community to join in. Every

master's and bachelor's degree program should include a cyber law and cybercrime course to raise public awareness. It is necessary to update educational programs in accordance with modern requirements. To raise awareness, the public should have access to a handbook explaining cyber laws and cybercrimes. An in-depth study is required to determine the true effects of cybercrimes on many sectors, including the economy, people of all ages, banks, government agencies, and the technology sector in general.

- Training on the use of technology and how to investigate must be given to FIA investigators.
- Cybercrime investigation officers need to be up to date on the latest technological developments.
- Pakistani people can be educated on how to protect themselves against cybercrime. Users must use precaution while providing sensitive information on social media sites; for example, they should not give out their passwords, locker numbers, or photos to complete strangers. Antivirus software that is up to date should be installed on the unused computers. When checking email, be careful just to look at recognized addresses; unsolicited messages can be disregarded. Installing security firewalls in businesses is essential to prevent illegal access and the use of credit cards online.
- The offence of cyber stalking under section 24 of the PECA is non cognizable offence in PECA 2016 which is required to be made cognizable offence for effective results in combating cybercrimes and cyber stalking.
- According to PECA 2016, all offences except Sections 10, 21, 22 are non cognizable and bailable, which requires to be revisited, reframed and enacted in order to make the offences cognizable and non bailable in terms of present need in order to combat the growing trends of cybercrimes and cyber stalking.
- The procedure of the complaint and registration of the complaint be made accessible to every nook and corner so that the victims may approach the Police stations easily and get the complainant magistrate.
- The minor girls being the most vulnerable become prey to the cyber criminals are required to educate through print and electronic media, seminars, secessions and group discussion at all levels.
- The data shows that the acquittal ratio is quite high which require to be dealt with and necessary trainings to the Cybercrimes Magistrate and investigation officers be given at international standard for evidence collections and new technological developments so that the culprits get booked as per law.

- The Cybercrime wings and circles may be stationed at district level so that the common and illiterate victims may approach the circle with much ease and little cost.

- The government of Pakistan has not framed any Cyber Policy till, which is need of the hour and may be framed within ultimate promptitude.

- Least but not the last, the research data reveals that the government Pakistan has not signed any treaty, Memorandum of Understanding (MOU) with face book (FB), WhatsApp, Snap chat, X, Instagram etc. and the authorities are not bound to share the data with the FIA authorities against the culprits keeping in view their own terms of policies of the users. Hence, the government is required to sign treaty or MOU with the aforementioned authorities in order to expedite the complaints effectively against the cyber criminals.

References

Agency fi. National response center for cybercrime 2021.

Ahlgrim BJM. Cyber stalking: Impact of gender, cyber stalker-victim relationship and proximity: The University of North Dakota; 2015.

Akhlaq M. Cybercrime in Pakistan: a study of the law dealing with cybercrimes in Pakistan. Pcl Student Journal of Law. 2021.

Akhtar S. Assessing the Cybercrime Legislation in Pakistan: A Comparative.2023.

Akram W, Kumar R. A study on positive and negative effects of social media on society. International journal of computer sciences and engineering. 2017;5(10):351-4.

Aleem Y, Asif M, Ashraf MU. The Prevention of Electronic Crimes Act 2016 And Shrinking Space for Online Expression in Pakistan. lkogretim Online. 2021;20(2).

Aleem Y, Tariq M, Umar M, Rafique MZ, Ashraf MU. Protecting Online Privacy in Pakistan. Pal Arch's Journal of Archaeology of Egypt/Egyptology. 2021;18(6):607-15.

Ali SI, Mohamed Yusoff Z, Ayub ZA. Legal research of doctrinal and non-doctrinal. International Journal of Trend in Research and Development. 2017;4(1):493-5).

Alkhalil Z, Hewage C, Nawaf L, Khan I. Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science. 2021; 3:563060.

Arshad Khan E. The prevention of electronic crimes acts 2016: An analysis. LUMS LJ. 2018; 5:117.

Bojilov M. Methods for assisting in detection of synthetic identity fraud in credit applications in financial institutions: CQ University; 2023.

Chawki M, Darwish A, Khan MA, Tyagi S. Cybercrime, digital forensics and jurisdiction: Springer; 2015.

Demetis DS. Breaking bad online: A synthesis of the darker sides of social networking sites. European Management Journal. 2020;38(1):33-44.

DeNardis L. The Internet in everything: Yale University Press; 2020.

Ernst N, Engesser S, Büchel F, Blassnig S, Esser F. Extreme parties and populism: an analysis of Facebook and Twitter across six countries. Information, Communication & Society. 2017;20(9):1347-64.

Express TT. Only 14 cybercrime convictions in five years. 2020.

Ghosh AK. An Exploratory Study on the Concept and the Form of Stalking as a Cyber Crime. Issue 5 Int'l JL Mgmt & Human. 2021; 4:668.

Gies SV, Piquero NL, Piquero AR, Green B, Bobnis A. Wild, wild theft: Identity crimes in the digital frontier. Criminal justice policy review. 2021;32(6):592-617.

Haider W, Ali A, Zubair M. Prevention of Electronic Crime Act, 2016: An Analysis of the Act’s Effectiveness in Controlling Misuse of social media in Pakistan. Journal of Educational Research and Social Sciences Review (JERSSR). 2023;3(2):48-54.

Halder D, Jaishankar K. Use and Misuse of Internet 2013.

Hedayati A. An analysis of identity theft: Motives, related frauds, techniques and prevention. Journal of Law and Conflict Resolution. 2012;4(1):1-12.

Horgan SL. Cybercrime and everyday life: exploring public sensibilities towards the digital dimensions of crime and disorder. 2019.

Jamshed J, Rafique W, Baig K, Ahmad W. Critical Analysis of Cybercrimes in Pakistan: Legislative Measures and Reforms. International Journal of Business and Economic Affairs. 2022;7(1):10-22.

Kemp s. Digital 2023: Pakistan Datar portal 2023.

Khan N, Shaikh A, Singh MVP. Understanding of cyber defamation and its impact: a critical analysis. Dogo Rangsang Res J. 2023; 13:168-73.

Kim B. Publication bias: A “bird's-eye view” of meta-analytic practice in criminology and criminal justice. Journal of Criminal Justice. 2022; 78:101878.

Lu C, Jen W, Chang W, Chou S. Cybercrime & cybercriminals: An overview of the Taiwan experience. J Compute. 2006;1(6):11-8.

Moriarty LJ, Freiberger K. Cyberstalking: Utilizing newspaper accounts to establish victimization patterns. Victims and Offenders. 2008;3(2-3):131-41.

Munir A, Gondal MT. Cyber Media and Vulnerability: A discourse on cyber laws and a probe on victimization of cybercrimes in Pakistan. Global Media Journal: Pakistan Edition. 2017;10(2):1-23.

Pyke A, Rovira E, Murray S, Pritts J, Carp CL, Thomson R. Predicting individual differences to cyber-attacks: Knowledge, arousal, emotional and trust responses. Cyberpsychology: Journal of Psychosocial Research on Cyberspace. 2021;15(4).

Regehr C, Burgess AW. Victims of Cybercrime: Sudbury; 2010.

Saini H, Rao YS, Panda TC. Cyber-crimes and their impacts: A review. International Journal of Engineering Research and Applications. 2012;2(2):202-9.

Singh MM, Bakar AA. A systemic cybercrime stakeholders' architectural model. Procedia computer science. 2019; 161:1147-55.

Smith SE. Threading the First Amendment Needle: Anonymous Speech, Online Harassment, and Washington's Cyberstalking Statute. Wash L Rev. 2018; 93:1563. 2018.

Statista. Most common forms of cyber stalking an ex or current partner worldwide as of January 2023.

Strauss A, Corbin J. Basics of qualitative research techniques. 1998.

The Global Village Online [Internet]. 2023.

Usman M. cybercrime: Pakistani perspective. Islamabad Law Review. 2017;1(03):18-40.

Venkiteswaran G. Let the Mob Do the Job: How Proponents of Hatred are Threatening Freedom of Expression and Religion Online in Asia. Association for Progressive Communications. 2017.

Woodlock D. The abuse of technology in domestic violence and stalking. Violence against women. 2017;23(5):584-602.