Journal of Media Horizons
ISSN: 2710-4060 2710-4052 Volume 7, Issue 3, 2026

EFFECTIVENESS OF THE PREVENTION OF ELECTRONIC CRIMES ACT 2016 IN COMBATING CYBER HARASSMENT IN PAKISTAN

Iqra Shahid

LLB, LLM

iqrashahid701@gmail.com

DOI: http://doi.org/10.5281/zenodo.19367743

Keywords

Article History
Received: 01 February 2026
Accepted: 17 March 2026
Published: 31 March 2026

Corresponding Author: *
Iqra Shahid

Abstract

The encroaching growth of digital technologies and internet connectivity has been of great importance as it relates to communication and social interaction in the global arena. The growing popularity of social media sites and online communication tools in Pakistan presents fresh opportunities in terms of economic development, sharing of information and participation of civilians in the country. Nevertheless, another drawback of this technological development is that it has given rise to other types of criminal behavior mainly cyber harassment, online stalking, identity theft and cyber blackmail. To cope with all these issues, the Prevention of Electronic Crimes Act 2016 (PECA) has been passed in Pakistan and puts in place a comprehensive legal framework to govern cyber offences.

This paper is a critical assessment of the effectiveness of PECA in counterattack cyber harassment in Pakistan. It analyzes the legal clauses of the Act, institutional enforcing mechanisms, and legal interpretation of cybercrime rules by judices. The paper also delves into the issues that have been related to enforcing cybercrime laws, such as institutional constraints, delays, digital illiteracy, and the law being used as a weapon. A comparative study of international regulatory framework, in particular, the General Data Protection Regulation (GDPR) is also conducted in order to point to possible changes. The argument in the article is that though PECA is a significant piece of legislation in regard to treating cyber harassment, the initiative is limited by weaknesses in structures and institutions. The paper has ended by giving legislative and policy recommendations that can be used to enhance governance of cybercrime and safeguard basic rights within the digital environment in Pakistan.

Introduction

The emergence of digital technologies has enhanced the basis of communicating, conducting business, and being sociable life of individuals. The internet penetration and the use of smartphones in Pakistan have exponentially impacted the amount of online interaction. Communication, entertainment, and professional networking have become the main means of communication of millions of people using digital platforms like Facebook, Instagram, and WhatsApp.

Although these platforms have both increased social connectivity and opportunities in the economy, it has allowed the development of new types of criminal behaviour. Social and legal issue in Pakistan has risen to a significant problem with cyber harassment. Online stalking, impersonation, spread of personal photographs as well as threats are quite common among victims via digital modes of communication.

Cyber harassment may result in serious psychological torture, loss of reputation, and social alienation. Online harassment affects women, newspeople and activists, especially. In most instances, the victims fear social stigma or they lack trust in the law enforcement agencies, hence they do not report cyber harassment.

Before 2016, the Paks legal system did not have a holistic framework in place to deal with cybercrime. The conventional criminal laws like the Pakistan Penal code were developed to govern physical crimes and were not appropriately adapted to a crime taking place in the digital space. Therefore, the Pakistani parliament passed the Prevention of Electronic Crimes Act 2016 to control the operations on the Internet and ensure that the victims of the online harassment receive judicial redress.

The adoption of PECA was an important milestone in the Pakistani legislation against cybercrime. The success of the legislation in dealing with cyber harassment is however questionable. Critics express that the law has multiple issues such as loopholes in its enforcement, institutional capability and fears of its provisions being abused.

This paper tries to critically evaluate the efficacy of PECA in fighting cyber bullying in Pakistan. It will discuss the legal context of the Act, assess the institutional enforcement strategies, review the case law, and highlight structural issues that have an impact on its implementation.

Idea and definition of Cyber Harassment.

Cyber harassment is a type of digital communication technologies that are used to intimidate, threaten, or harm people. It is one of the types of online abuse that can take place in social media, messaging apps, email, or any other digital communication framework.

Cyber harassment may take several forms including:

Cyber stalking
Online defamation
Digital impersonation
Non-consensual sharing of private images
Threatening or abusive messages

Digital blackmail and extortion

Cyber harassment, unlike in case of traditional forms of harassment, may be anonymous and it can reach a broader network of people via digital networks. It is also associated with the fact that most content posted online is here to stay and thus and remains harmful information which can damage the reputation forever.

Moreover, cross-jurisdictional aspects are often present in cyber harassment as the individual violating can be geographically far apart. The nature of these characteristics renders cyber harassment highly challenging to control by using the traditional criminal law means.

The Pakistani Cybercrime Legislation.

The Prevention of Electronic Crimes Act 2016 is the major federal legislation in Pakistan in connection with cyber crimes. The Act was passed in order to accord legal validation to cybercrime and develop investigative and prosecutorial policies to digital crimes.

The Act makes criminal offences in relation to cyber offences a broad area such as:

Intrusion to information systems.
Electronic fraud
Identity theft
Cyber stalking
Online harassment
Electronic forgery

Application of Cybercrime Laws in Pakistan: Comparison with the United Kingdom.

Communication, commerce, and government are changing globally with the growth of digital technology. But it has also helped the creation of new crimes involving cybercrime such as hacking, identity theft, cyber harassment, online fraud and digital blackmail. The world has countered this through governments enacting cybercrime laws to control internet behaviour and save people under the effects of digital attacks.

The Prevention of Electronic Crimes Act 2016 (PECA) was part of the efforts by Pakistan to deal with cyber offences and provide a legal framework, in which the digital activities could be regulated. On the same note, the United Kingdom has come up with a detailed cybercrime regime with the

inclusion of law like Computer Misuse Act 1990, and Data Protection Act 2018.
This part looks at the application of cyber laws in Pakistan and how they compare with the law of the United Kingdom so as to determine their effectiveness.

Cybercrime Laws in Pakistan
The cybercrime law is mainly regulated by the Prevention of Electronic Crimes Act 2016 in Pakistan, which has been adopted in order to control cyber crimes and provide a mechanism of enforcing them..

Key Features of the Law
The Act criminalizes various forms of cybercrime, including:
Unauthorized access to information systems
Identity theft
Electronic fraud
Cyber stalking
Online harassment
Digital impersonation
Electronic forgery
Investigative agencies are also given the mandate by the law to gather digital evidence and prosecute criminals.

Enforcement Authorities
In Pakistan, the task of enforcing the laws relating to cybercrime is done by the cybercrime wing of the Federal Investigation Agency (FIA).
The roles of the FIA are:
Resolution of complaints caused by cybercrime.
Digital forensic investigation.
Determining the identity of those who commit cyber crimes.
Criminal prosecution.
They have also instituted special cybercrime courts to deal with such cases in the Act.
Implementation as a challenge.
Despite the fact that the legislation offers a legal framework on which cybercrime can be addressed, there are a number of challenges constraining its efficacy.

Lack of Institutional Capacity.
The Federal Investigation Agency cybercrime wing has problems of inadequate trained investigators, digital forensic specialists, and technological tools.

Low Public Awareness
A large number of citizens do not know the legislation on cybercrime or how to report on any online harassment.

Procedural Delays
Investigation of cybercrime may engage elaborate and intricate digital proof, thus postponing the prosecutions.

Concerns Regarding Misuse
The opponents believe that some clauses in the law can be employed to curtail the freedom of expression or in order to suppress political dissent.
The United Kingdom Laws on Cybercrime.
The UK has constructed one of the best legal frameworks of cybercrimes world over. A number of laws governing cybers crimes do exist.
Computer Misuse Act 1990
The main law on cybercrime in the United Kingdom is the Computer Misuse Act 1990. The Act criminalizes:
Illegal entry to computer systems.
Access to the data that should not be accessed.

Cyber sabotage and hacking
The legislation has been revised to meet the new cyber threats like malware attacks and denial- of-service attacks.
Processing Data Protection and Privacy Laws.
Another law that regulates cyber activities in the United Kingdom is the Data Protection Act 2018 that implements the inception of the General Data Protection Regulation.
The essence of the laws is to safeguard the personal information and make sure that the organizations handle digital information in a responsible manner.

Enforcement Institutions
In the United Kingdom, the enforcement of cybercrime is done through specialized agencies such as the National Crime Agency.

UK has also developed highly developed digital forensic units and dedicated teams to investigate cybercrimes so as to effectively hash out internet crimes.

Pakistan and the United United Kingdom.

An analysis of Pakistan and the United Kingdom shows that they have a number of differences regarding cybercrime and regulation systems.

Legal Framework

The major law that is used to control cyber offences in Pakistan is the Prevention of Electronic Crimes Act 2016.

Conversely, the United Kingdom has devised an all-inclusive system of cybercrime laws comprising of various laws among them the Computer Misuse Act of 1990 and the Data Protection Act of 2018. It is a multi-layered structure that enables the UK to control data protection and cybercrime.

Institutional Capacity

The UK boasts of superior technological infrastructure as well as dedicated cyber criminology units.

Comparatively, Pakistan enforcement agencies have their resources limited and they can hardly investigate intricate cyber crimes.

Awareness and Digital Literacy in the Community.

Between the domestic factors, the digital literacy programs across the United Kingdom have ensured that the populace is much more informed about cybercrime laws in the country.

In Pakistan, only a few people have awareness that helps to minimize reporting of cyber offences.

Copyright of Digital Rights.

The UK jurisprudence is very protective of privacy and data rights by law using Data Protection Act 2018 and the General Data Protection Regulation.

The cybercrime policy of Pakistan is concerned more with criminal punishments than wider internet controls and digital safeguards.

Pakistan Lessons based on the UK Model.

Pakistan can further enhance their system of cybercrime by following some of the practices that are practiced by the UK system.

Institutional Strengthening

Enhancements in the technological capability and plan of the Federal Investigation Agency.

Data Protection Legislation.

Conceptualizing tougher data protection regulations on the lines of the General Data Protection Regulation.

Public Awareness Campaigns

Encouraging online literacy and sensitisation of online cybercrime reporting processes.

Judicial Training

It should train judges and prosecutors, who handle cybercrime cases, with specific training.

Compared to the challenge of cybercrime, modern legal systems are faced with a big challenge. The enactment of the Prevention of Electronic Crimes Act 2016 constitutes an important move that Pakistan has made towards formulating the law that will regulate cyber offences. Nevertheless it is the weakness of the law as it has been implemented owing to institutional limitations, a lack of social awareness and enforcement.

Conversely, the United Kingdom has formulated an extensive cybercrime regulatory framework in its legislations like the Computer Misuse Act 1990 and the Data Protection Act 2018. The UK system enjoys a high degree of institutional capacity, high level of technological infrastructure, and a formidable data protection system.

The effectiveness of cybercrime laws can be improved by increasing the effectiveness of enforcement institutions, digital literacy, and the implementation of tougher regulatory mechanisms in Pakistan, which will offer more protection to individuals against harm on the Internet.

A number of the provisions of the Act deal directly with cyber harassment.

Article 20:A Crimes against the dignity of a Natural Person.

Section 20 proclaims the distribution of information via digital systems, which damages the esteem or respect of a person. The given provision

deals with online defamation and reputational damage that is committed by the use of digital means.

1. The offence of incest, the offence of pregnancy, and the offence of rape, namely, adultery, are those covered by the law that convey to the perpetrator shame before the community and the rebirth following a single marriage, resulting in his/her near annihilation after each crime.<|human|>21: Offences Against Modesty. They are the offence of incest, the offence of pregnancy, the offence of rape, that is, the adultery, whereby the law teaches him rebirth after single marriage, and his near annihilation by

Section 21 makes it an offense to share or threat to share intimate pictures or videos without authorization with the view to humiliate and blackmail victims. Such a clause is especially essential in dealing with cyber harassment on the basis of gender.

Section 24: Cyber Stalking

Article 24 outlaws recurrent online communication, surveillance of online activities as well as spreading of personal details aiming at intimidating or harassing individuals.

All these provisions bring legal ground on prosecution against cyber harassment offences in Pakistan.

A comprehensive legal argument of any loopholes in the application of cyber laws in Pakistan as follows is suitable to use in an attractive LLM study or article, or even assignment.

Wrapping up FIA role in fighting Cybercrime.

In Pakistan, the Federal Investigation Agency (FIA) has a key role to play in the prevention, investigation and prosecution of cybercrimes, through its Cyber Crime Wing (CCW).

Investigating Cyber Offences: The reality is that a greater number of crimes in the 21 st Century are perpetrated via the Internet compared to previous centuries.<|human|>Investigation of Cyber Offences: The fact of the matter is that more crimes in the 21 st Century are being committed over the Internet than had been done in earlier century.

FIA is involved in investigating cybercrime complaints submitted by people. Offences may be reported by the victims using:

FIA Cyber Crime Reporting Centres

|human|>Cyber Crime Reporting Centres FFIA.

Online complaint portals

Direct visits to FIA offices

The agency gathers the digital evidence, traces the IP addresses, and immerses the suspects via the use of the forensic methods.

Digital Forensics

The FIA has sophisticated digital laboratories that are designed to examine both computers, mobile phones, servers, and storage devices. Cybercrime cases depend on the role of digital evidence to prove the offender in court.

The prevention and public awareness is done in 4.3.

FIA does awareness campaigns to inform the community about online security, cyber fraud, and good internet behavior. These campaigns contribute to victimization minimization and especially women and the young internet users.

International Cooperation

Cybercrime is commonly characterized by criminals in different nations. The FIA works in association with other organizations based internationally like:

Interpol

International Telecommunication Union.

Such collaboration aids in monitoring global online criminal groups.

Reproductive health might be included here too as it constitutes a crucial element of a healthy pregnancy or childbirth.<|human|>4.5 Prosecution of Cyber Offenders.

Investigations are finalized by FIA who then delivers cases to the courts that are set up by PECA. These are courts that deal with the trials about cybercrime and punishments are fines and jail term.

Obstacles that FIA has encountered in the fight against Cybercrime.

The Federal Investigation Agency has a significant value, but it has a range of challenges:

Low level of technical capacity and qualified human resource.

The growing use of the internet is resulting in increasing numbers of cybercrimes.

Problems in jurisdiction in cases of foreign servers crimes.

Social ignorance on reporting cyber offences.

The manner in which PECA has been criticized as being prone to abuse and restriction of the freedom of expression.

These hurdles point to the preparation of greater institutional strength and legalization.

Recommendations

In a bid to make cybercrime control effective in Pakistan:

Grow Technical training and recruitment of FIA in Cyber Crime Wing.

Enhance digital forensic.

Review the Prevention of Electronic Crimes Act 2016 to accommodate the emerging cyber threats.

Enhance global collaboration of transnational investigations.

Implement country-wide digital literacy technologies..

Conclusion

One of the most critical concerns of the digital age is being the cybercrime. The Federal Investigation Agency is very instrumental in the implementation of cyber laws in Pakistan through the Prevention of Electronic Crimes Act 2016. Although the FIA has been encroaching much to do in tracking and prosecuting cyber criminals, the legal frameworks, technological capability as well as community awareness must be enhanced to ensure that the future achievements in curbing cybercrime.

PERA:

Cybercrime is one of the most significant legal and social issues in Pakistan alongside a widespread development in the use of the internet and digital communication. The government has tried to overcome these difficulties by implementing the Prevention of Electronic Crimes Amendment 2016 (PECA), which gives the main legal framework of the regulation of online criminal activities like hacking, cyber harassment, identity theft, and on-line fraudulent acts.

The law is a great move towards controlling cybercrime, even though its application exercises a number of loopholes involving law, institutions, and the process. These flaws lower the efficiency of the cybercrime enforcement and deny the victims an opportunity to receive justice.

Limitations of the institutional capacity.

Poor institutional capacity of the agencies enforcing the cyber laws is one of the greatest problems in realizing cyber laws in Pakistan.

Cybercrime division of the federal investigation agency wages cyber crimes under PECA. The agency however experiences a number of operation constraints such as:

Lack of trained investigators of cybercrime.

Inadequate digital forensic labs.

Absence of high technological equipments.

Lack of enough personnel in the area offices.

These restrictions make cybercrime investigations less effective and in most cases it leads to further processing of the cases.

Absence of Digital Forensic Knowledge.

Investigation of cybercrimes needs to pass a specialized skill of digital forensics, in order to track IP addresses, restore deleted information, and analyze electronic evidence. Nevertheless, most of the investigators are poorly trained in digital forensic methods.

Due to it, prosecution will have problems gathering viable digital evidence, undermining cases in courts.

Jurisdictional Challenges

In a lot of cases cybercrime is cross-border involving the offenders being based in various nations. This poses challenges legally to the Pakistani authorities.

Cyber offences are often globalized networks and therefore, the investigation of these crimes involves cooperation among all international countries and mutual legal support. Nonetheless, the ways of enforcing cybercrime in Pakistan do

not have upscale international coordination frameworks.

Delays of the Procedure of Investigation and Prosecution.

The other enormous loophole that is present in enforcing the specific cyber laws is that the investigation and courtwork becomes slow.

CRM inquiries may include:

Complex digital evidence

More than one suspect in other jurisdictions.

Forensic technological examination.

The factors could postpone the investigation process. Besides, the overall slowdown of prosecution of cybercrime cases is further exacerbated by the general backlog in courts.

Weak Springboard of Cybercrime Legislation.

Many victims of cyber harassment do not know their rights under the Prevention of Electronic Crimes Act 2016. Not all people are aware of the way they can report cyber offences or make complaints to the concerned authorities.

The lack of digital literacy and awareness among people lowers the number of reported incidences of cybercrimes and this reduces the efficiency of cyber law.

Undercyber harassment is reported.

The victims are usually deterred against reporting the cases of cyber harassment due to social stigma especially the women. The victims are afraid of the bad name or fear of being socially ostracized in case they move to court.

It is one of the cultural barriers leading to underreporting of cybercrime cases and thus challenges police to tackle the entire extent of the issue.

Imprecise and general law clauses.

Some clauses of the Prevention of Electronic Crimes Act 2016 have been said to be too broad or too vague. As a case in point, online speech provisions can be construed in a manner that will limit freedom of speech.

Scholars of law and activists of digital rights claim that ambiguity in statutory language can cause the inconsistency of law application.

Risk of Misuse of Cyber Laws

The other issue is associated with misuse of cybercrime laws that may be directed at journalists, activists, or those political figures, who oppose them. The critics note that broad clauses can be used to take up people

who post different opinions against them on the Internet.

This kind of abuse may destroy trust in cybercrime laws.

Weak Cybercrime Infrastructure.

Some cybercrime reporting centres in Pakistan are rather few in perspective of the huge number of internet users. In the rural communities, there is a high number of victims not having access to computer crime reporting services.

Such infrastructural deficiency renders reporting and seeking legal redress in place of reporting of offences difficult to the victims.

Lack of Co-ordination between Institutions.

Reducing cybercrime crimes is a complicated issue that cannot be achieved without collaboration between different organizations such as the law enforcers, communication regulators, and the courts.

Nonetheless, Pakistan has a low level of institutional coordination. Cybercrime investigations are usually hampered by the delay in sharing information and administrative processes.

Remarks:

Even though the Prevention of Electronic Crimes Act 2016 offers a crucial legal framework to control cybercrime in Pakistan, its application is not as effective as it could have been due to some loopholes in its application. The constraints of institutional capacity, the lack of digital forensic skills, procedural latency, the ignorance of the population, and the issue of jurisdiction remain the obstacles to the efficient enforcement.

To deal with such loopholes, broad reforms in the area such as reinforcement of investigative capacity, building of cybercrime infrastructure, augmenting digital literacy, and clarity in the legal provisions are necessary. These reforms will help Pakistan improve the efficiency of the cybercrime

regulatory regime to a greater degree of safeguarding people against cybercrimes.
The cybercrime wing of the Federal Investigation Agency (FIA) mainly executes the enforcement of the cybercrime laws. The agency deals with the investigation of complaints against cybercrime and criminal prosecutions.

Cyber harassment may be reported by the victims by:
Online complaint portals
Cybercrime centres that report.
Electronic evidence to the investigative department.
The section of cybercrime courts has also enhanced the judicial reaction to the cybercrime cases.
But the efficiency of these enforcing mechanisms is mostly related to the organizational capability of law enforcement organizations, and access to digital forensic capabilities.
Cyber Harassment- Statistical Trends in Pakistan.
Over the last ten years in Pakistan, cyber harassment has grown tremendously with the ongoing use of the internet, itself and its smartphones.
In accordance with reports provided by the Federal Investigation Agency, thousands of complaints on cybercrime are registered every year. Quite a high rate of these complaints is related to online harassment, impersonation, and blackmail.
Correspondingly, the Digital Rights Foundation based Cyber Harassment Helpline has continued to take an upsurge in the lamentations in connection with the matters of online harassment, especially in women and young computer users.
These figures indicate that cyber harassment is a prevalent social ills in the society that needs to be successfully controlled through the law.

Judgment and Case Law.
Judiciary in Pakistan has been significant in interpretation of cybercrime laws and solving cases of cyber harassment.
The Lahore High Court, in Humaira v State (2019 YLR 2456), pointed out that cyber harassment may result in serious psychological effects and reputational losses. The court affirmed the guilt of the accused and once again put into perspective the need to enforce the laws addressing cybercrimes.
Equally, in Sadia Arshad v Federation of Pakistan (PLD 2018 Islamabad 243), the court identified the weakness of women against online harassment and called on the officials to beef up enforcement protocols.
With these court rulings, there is an evident rise in the acceptance of digital harm in Pakistani law.

Measuring the Performance of PECA.
Cyber Harassment should be legally recognized.
Among the major accomplishments of PECA, there is the establishment of cyber harassment as a criminal offence. Before the introduction of the Act, victims previously had limited legal redress to internet abuse.
The legislation has established a legal system, which the victims can use to pursue justice.
Infrastructure Design Cybercrime Investigation.
Presence of cybercrime investigation section in the Federal Investigation Agency has enhanced the capability of the law enforcing bodies to inspect online crimes.
Upon the introduction of digital forensic tools, the investigators are now able to trace the IP addresses and locate the online perpetrators.

Judicial Awareness
The Pakistani courts have started to realise the gravity of cyber harassment and started to interpret the cybercrime laws in a manner that understands the damage done by cyber harassment.

Difficulties during Implementation.
PECA has a number of challenges despite the strengths it possesses in legislative aspects.

Facilities Deficiencies.
The Federal Investigation Agency has a cybercrime wing that has few resources and staff. A lot of investigators do not have specialised training in the area of digital forensics.

Procedural Delays
Individual cases are likely to serve as hindrances to the speed in which cybercrime can be prosecuted

because of the complicated technical nature of investigations.

Lack of Public Awareness

This is because many citizens are still not aware of the laws related to cyber harassment as well as how to report cybercrime.

Concerns Regarding Misuse

Others claim that a few of the provisions in PECA have ambiguous words that can be abused by those in authority to limit freedom of expression.

Comparative Analysis

Most countries have internationally passed detailed laws on cybercrime, which blend a criminal sanction with regulatory protection.

As an illustration, the European Union has set up powerful standards of data protection, namely the General Data Protection Regulation that focuses on privacy protection and accountability.

The regime in cybercrime in Pakistan resorts more to criminal punishment as opposed to preventative regulatory intervention compared to such systems.

Reform Proposals

Some improvements can be made in order to improve cyber harassment laws in Pakistan.

Enhancing the investigative power of the Federal Investigation Agency.

Increasing cybercrime reporting systems.

Specialisation training of law enforcement agencies.

Educating the population on laws regarding cybercrime.

Proposing legal protection against misuse.

Concluding remarks:

The Prevention of Electronic Crimes Act 2016 can be viewed as one of the major legislative attempts to control the cybercrime and prevent the online harassment in Pakistan. The Act has established a necessary law system to prosecute cyber crimes and safeguard the victims of cyber abuse.

Nevertheless, its effectiveness is still constrained by enforcement issues, weaknesses in the institution, and questions of misuse. To create an efficient cybercrime regulatory environment, it is important to enhance the ability of investigations, public awareness and the protection of the constitutional rights.

Since the digital landscape is still developing in Pakistan, a moderate stance of enforcement of the law, technological understanding, and security of the digital rights will be required to confront the issue of cyber harassment.

References

Legislation

Prevention of Electronic Crimes Act 2016

Cases

Humaira v State (2019 YLR 2456)

Sadia Arshad v Federation of Pakistan (PLD 2018 Islamabad 243)

Reports and Books

Digital Rights Foundation, Cyber Harassment Helpline Report (2022)

Muhammad Amir Rana, Cybercrime and Digital Security in Pakistan (Institute for Policy Studies 2020)

Federal Investigation Agency, Cyber Crime Wing Annual Report (2023)

International Instrument

General Data Protection Regulation (EU) 2016/679