DOI: https://doi.org
Journal of Global Social Transformation
Journal homepage: https://rjsaonline.org/index.php/JGST

Legal Challenges in the Prosecution of Cybercrimes Under the Prevention of Electronic Crimes Act 2016

Saira Hassan[1], Muhammad Ali Muzammil[2]
[1]Faculty of Law, University of the Punjab,
[2]School of Law, Lahore University of Management Sciences
Email: sairahassan55@ymail.com

ARTICLE INFO

Received:
November 20, 2025
Revised:
December 19, 2025
Accepted:
January 02, 2026
Available Online:
January 13, 2026

Keywords:
PECA 2016, prosecution of cybercrime, prosecution of virtual evidence, criminal, prosecution, Pakistan, qualitative studies, crook regulation, cyber regulation reform.

Corresponding author:
sairahassan55@ymail.com

ABSTRACT

The gift qualitative studies tested the felony problems the prosecution of cybercrimes faces in Pakistan thru the Prevention of Electronic Crimes Act 2016 (PECA). The have a look at become carried out with the assist of a combination of a doctrinal and qualitative method to criminal evaluation and empirical research of fourteen prison practitioners, judges, cybercrime investigators, and felony pupils who participated withinside the take a look at with the assist of purposive and snowball sampling at some point of Pakistan. Interpreted thematic evaluation of the interview facts changed into triangulated with the doctrinal evaluation of statutory provisions, pronounced judgments and secondary prison literature. There have been 5 predominant thematic regions of challenge, namely, evidentiary demanding situations and inadequacies in virtual forensics; conceptual ambiguities and shortcomings in legislative drafting; complexities in jurisdiction and enforcement demanding situations; procedural due technique lines and demanding situations in essential rights; institutional capability troubles withinside the crook justice system. The outcomes suggest that despite the fact that PECA 2016 is a groundbreaking legislative alternate withinside the virtual criminal surroundings of Pakistan, the act is full of interpretative ambiguities, enforcement loopholes, and institutional shortcomings which might be systematically hindering the powerful prosecution of cybercrimes. The studies affords novel empirical and theoretical contributions to the nonetheless enormously new frame of studies at the regulation of cybercrime withinside the Global South and progresses precise tips on the subject of legislative extrade, ability development, and procedural modernization.

Introduction

The creation of our on-line world as a area of human motion has led to new kinds of damage that undermine the conceptual foundation and the procedural tactics of the traditional crook regulation. Crime with a pc factor Cybercrime, which include the unauthorized get admission to to laptop structures, robbery of information and facts, and different offenses perpetuated via way of means of on line means, does now no longer comply with territorial lines, and leaves strains which can be risky and technically challenging, and maximum probably engages actors whose identities are deliberately hidden through the layers of on line anonymity. These elements make cybercrime appreciably exceptional to standard crime and require unique legislative, investigative and prosecutional reactions which maximum prison structures which includes in Pakistan are but to establish.

The Prevention of Electronic Crimes Act 2016 (PECA) is the primary regulation of the USA that has been enacted to criminalize and prosecute cybercrimes. Before PECA, the regulation on cybercrime in Pakistan became a haphazard

association made below the Electronic Transactions Ordinance 2002 and popular crook regulation- a framework this is normally recounted to be poorly appropriate to cope with the dimensions and complexity of present day virtual crime (Waseem, 2017). PECA 2016 integrated a listing of all styles of cybercrime offences, created unique investigative and prosecutorial techniques, a unique cybercrime reporting and research enterprise withinside the Federal Investigation Agency (FIA), and positioned unique jurisdiction in unique cybercrime courts. This way, it changed into the maximum vital amendment of the virtual crook regulation in Pakistan for the reason that inception of the net age.

Nevertheless, regardless of its legislative ambition, PECA 2016 has acquired regular grievance amongst felony practitioners, civil society groups, human rights organizations, and felony teachers because of its indistinct and over large definition clauses; and its cappotential for use as a device of political suppression and curtailment to loose speech (Mustafa, 2021; Rahman, 2022). In heredity to the mainstream of such concerns, the crook prosecution of cybercrimes beneathneath PECA has been characterised with the aid of using huge problems via every segment of the crook procedure, encompassing research to conviction, in addition to constitutional and human rights needs that need to govern any crook procedure.

The frame of educational studies into cybercrime regulation in Pakistan is pretty restrained compared to the massive quantity of studies on cybercrime regulation in evolved international locations just like the United States, the UK and the European Union. Pakistani scholarship has been willing toward descriptive evaluation of the doctrines in PECA, and has now no longer been empirically worried withinside the sensible criminal problems concerned in operating in the device. This paper tried to fill that hole via the synthesis of doctrinal interpretation of PECA 2016 and judicial interpretation with qualitative empirical information gathered thru semi-based interviews with lawyers, judges, cybercrime investigators, and criminal pupils. This two-sided methodological method allowed a delicate, grounded narrative of the felony troubles that cybercrime prosecution faces which transcends the textual content of the regulation to the realities of the criminal exercise withinside the Pakistani cybercrime courts.

The studies questions shaped the premise of the look at and had been as follows: What are the principle criminal problems in prosecuting cybercrimes below PECA 2016? What is the effect of evidentiary and forensic issues at the end result of a cybercrime prosecution? How do the definitional and interpretative uncertainties of PECA 2016 gift prison uncertainty? What may be completed to institute institutional and procedural adjustments to decorate prosecution of cybercrime in Pakistan? These questions, and their answers, now no longer simplest have an educational scholarship implication however additionally a realistic improvement of the cybercrime justice machine in Pakistan, and certainly the venture as an entire of growing powerful and rights-respecting cybercrime prison structures withinside the Global South.

Literature Review

The International Cybercrime Law Enforcement Environment

This is due to the fact the lawmaking reaction to cybercrime has turn out to be a feature region of situation in comparative crook regulation scholarship withinside the final twenty years. The first and maximum famous worldwide treaty on cybercrime, the Budapest Convention on Cybercrime (2001) of the Council of Europe, has furnished a fixed of great offences, procedural powers and worldwide cooperation mechanisms which has turn out to be the template utilized in maximum nations withinside the global to codify cybercrime (Clough, 2015). Budapest Convention has despite the fact that been criticized as it isn't extensively followed past the Global North, and its procedural clauses, as a few pupils argue, awareness at the performance of regulation enforcement on the price of privateness and due method rights (Daskal, 2018).

Researchers have located that there are some of not unusualplace varieties of impediment that plague the prosecution of cybercrime irrespective of the jurisdiction. The works of Wall (2007) have defined cybercrime as posing a key mission to the policing creativeness because of its international scope, its technical nature and the incapacity to decide the crook conduct of positive people withinside the our on-line world. Brenner (2010) has set up a wide typology of criminal troubles created through cybercrime which includes the jurisdictional fragmentation, insufficiency of antique evidentiary policies to the virtual proof and the battle among the powerful research and the safety of civil liberties. Casey (2011) made a unique emphasis on virtual forensics claiming that the integrity, admissibility and probative fee of virtual proof pose a unique trouble that can't be absolutely treated with the aid of using the modern felony structures.

The felony literature on cybercrime in growing and rising economies has additionally installed different structural troubles which might be introduced approximately with the aid of using useful resource limitation, institutional underdevelopment and virtual divide. As Chawki et al. (2015) noted, the rules on cybercrime has been followed through many growing international locations following the Western styles with out sufficiently thinking about the institutional, infrastructural, and social situations below which those legal guidelines are alleged to be enforced, which ends up in the adoption of technically superior legal guidelines, however nearly not possible to enforce. Ibrahim (2016) diagnosed the unique hassle of prosecutors

in jurisdictions with decrease virtual forensic functionality wherein the technical elements of cybercrime research are regularly past the revel in degree in lots of instances.

PECA 2016: Architecture and Critical Assessment of Legislation

PECA 2016 is an inclusive attempt to cope with the whole gamut of cybercrimes threats to the ever-evolving linked Pakistan society. The unauthorized get admission to to records structures (Section 3), unauthorized copying or transmission of facts (Section 4), interference with data structures (Section 5), digital fraud (Section 9), digital forgery (Section 10), misuse of encryption (Section 11), cyberterrorism (Section 10A), on-line harassment (Section 24), cyberstalking (Section 24A) and dissemination of It additionally offers the FIA huge investigative authority (inclusive of seek and seizure of digital equipment, real-time visitors data and interception of communications with judicial consent).

The provisions of PECA had been explored through criminal pupils with the aid of using looking doctrinal critique. According to Mustafa (2021), the definitional clauses of the Act had been characterised through each vagueness and overbreadth that reasons excessive stages of interpretative ambiguity. Section 20, which makes it against the law to unfold facts this is fake and that is meant to result in fear, panic, sickness or unrest through a collection of residents has been a factor of contention, with critics mentioning that it has elastic language and may be used in opposition to political dissidents, journalism and activism with the aid of using civil society. In Muhammad Younis v. Federation of Pakistan (2021), the Supreme Court of Pakistan diagnosed the constitutional conflicts worried withinside the speech-associated offences of PECA, however did now no longer cross as some distance as to invalidate the indignant provisions.

In a initial assessment of the implementation troubles of PECA, Waseem (2017) mentioned 5 essential spheres of problems that included: the absence of skilled judicial and prosecutorial staff, insufficiency of virtual forensic infrastructure withinside the FIA, the intricacy of cross-border cybercrime investigations, the case backlog in committed cybercrime courts, and the dearth of regular sentencing legal guidelines to use to cybercrime Rahman (2022) revised this look at and observed that, even after years of enjoy in implementation, maximum of those troubles had been nonetheless in large part unattended because of the systemic institutional inertia, however now no longer always because of technical and aid limitations.

Digital Evidence: Lawful and Forensic Aspect

There are some of specific demanding situations of virtual proof to the prison regimes of definitely any jurisdiction, but it's far in particular in such structures as the only in Pakistan that the institutional infrastructure that helps virtual forensics is withinside the early stages of its improvement. According to Mason and Seng (2017), 3 crucial functions of virtual proof that make it stand out of the conventional bodily proof are its intangibility, reproducibility, and fragility. Contrary to a bodily proof, virtual proof is withinside the shape of a sample of electromagnetic charges, which may be flawlessly duplicated, without difficulty modified, and speedy destroyed, and adjustments can regularly be invisible to a layman.

A complex or even conflicting gadget of legislative acts and judicial precedents has regulated the admissibility of virtual proof in Pakistani courts. The Evidence Act (Qanun-e-Shahadat Order 1984) (previous the virtual era) has no digital proof provisions whatsoever, which has supplied an opening that PECA and the Electronic Transactions Ordinance 2002 have sought to address. PECA consists of segment forty one that lets in digital proof to be admissible supplied it's far authenticated, however the instances beneathneath which this is executed are disputed and range throughout numerous cybercrime jurisdictions (Shah and Afridi, 2020).

The difficulty of virtual forensic understanding as a top notch bottleneck withinside the prosecution of cybercrime has attracted the focal point of students throughout the global. In Pakistan, the FIA Digital Forensics Laboratory in Islamabad is the critical institutional repository of forensic knowledge, that is normally diagnosed to be insufficient to deal with the quantity and complexity of cybercrime instances despatched to the laboratory (Hussain and Bashir, 2021). Chain of custody necessities of virtual proof, which can be crucial to expose that proof has now no longer been altered in the course of the time among seizure and presentation earlier than court, are regularly violated due to the fact poorly skilled investigators do now no longer realize the forensically sound series and protection methods.

Basic Rights, Freedom of Expression and PECA

The warfare among the enforcement provisions of PECA and the primary rights furnished below the Constitution of Pakistan 1973 has been an trouble below which a good sized quantity of felony scholarship and remark with the aid of using civil society has been expressed. Articles 14, 16, 17, 18, 19, and 19A of the Constitution steady rights of dignity, assembly, association, trade, loose expression, and get admission to to facts respectively, rights that the speech-associated and provision of content material in PECA had been contended to endanger. The Human Rights Commission of Pakistan, the Pakistan Bar Council, and different worldwide bodies, along with the Amnesty International and the Human Rights Watch, have

additionally expressed grievance over the utility of the PECA provisions to goal the activists, journalists, and different political opponents (Human Rights Watch, 2021).

Ali (2022) achieved a near constitutional exam of speech offences, that are discovered in PECA, with the aid of using declaring that the proportionality criterion, as expressed with the aid of using the Supreme Court withinside the case of Benazir Bhutto v. Federation of Pakistan (1988), and similarly instances, should call for that any ban on unfastened expression be restricted, have a legitimate purpose, and be applied withinside the least restrictive way possible. According to Ali, a few provisions of PECA do now no longer byskip this test, the maximum distinguished being Sections 20 and 37, which criminalize speech that's in some way fake, obscene, or towards the dignity of Islam with out sufficiently defining the boundaries of those classes or installing area procedural protections towards their misuse.

Methodology

Research Design and Philosophical Orientation

The research design followed in this study was qualitative research design which incorporates the doctrinal legal analysis and empirical qualitative research design using semi-structured interviews. The doctrinal aspect was systematic interpretation of the text of PECA 2016, the statutory provisions associated with it, such as the Code of Criminal Procedure 1898 and the Qanun-e-Shahadat Order 1984, as well as judicial interpretation of the provisions of PECA and reports of judicial decisions. The analysis formed the legal context under which the empirical results were analyzed and put into context.

The empirical part was based on the interpretive epistemological orientation, which acknowledges that the legal issues that come with the prosecution of cybercrime under PECA are not technical phenomena to be quantified but socially constructed realities which are produced, experienced and disputed by the legal actors inhabiting the cybercrime justice system of Pakistan. This orientation is aligned with the prevailing tradition in the sociolegal research that focuses on the gap between law in the books and law in action and adopts the views of legal actors as privileged knowledge sources regarding how legal norms work in practice (Banakar and Travers, 2013).

Sampling and Selection of participants

The combination of snowball and purposive sampling techniques was used to recruit the participants. Purposive sampling was used to select the participants to identify those with direct professional experience that was pertinent in the context of prosecution of cybercrimes under PECA 2016, such as practicing criminal lawyers with experience in prosecuting cybercrime cases, judges who preside over a specific court that concerns cybercrimes, investigators attached to the National Response Centre of Cyber Crimes under the FIA, and legal scholars in the field of information Snowball sampling was considered to get to other participants via professional referrals so as to recruit those whose knowledge or experience could be of special interest as an informant but who may not have been accessible using purposive identification.

Fourteen participants were eventually recruited, including four practicing criminal lawyers, three cybercrime court judges, four FIA cybercrime investigators and three law faculty members with an expertise in cyber or criminal law. This piece offered insights into the institutional spectrum of cybercrime prosecution and so, facilitated triangulation of the participants categories and minimized the possibility of results being biased to the partisan view of any given group of professionals. The sample was identified in Islamabad, Lahore, Karachi, and Peshawar, which offered geographic representation of the regional difference in the application and experience of PECA.

Data Collection

Each participant was interviewed using semi-structured interviews, and the individual interviews took a duration of between thirty and ninety minutes. The interview guide was created according to the research questions and the current literature and included the thematic areas as follows: the overall evaluation of PECA 2016 as a legal tool to prosecute cybercrime; particular problems that have been faced in the investigation, evidence collection, and prosecution of cybercrime cases; the experiences related to the admissibility and probative value of digital evidence; the perception of the judicial capacity and familiarity with digital The semi-structured format allowed covering these areas in a systematic manner and at the same time allowed the participants to bring up other issues that were not envisaged by the interview guide.

The interviews were carried out face to face or through secure video conferencing, based on the location and the preference of the participants. All the interviews were recorded using audio and transcribed verbatim with the consent of the participants. All research outputs were given pseudonyms to the participants to maintain their privacy. The transcripts of the interview were complemented with a reflexive research diary, which was kept during the fieldwork period, and documented the observations of the researcher, the analytical insights, and thoughts about the dynamics of the interview process.

Data Analysis

As the primary data analysis approach, the thematic analysis was used in accordance with the six-phase process described by Braun and Clarke (2006, 2022): familiarization with the data, initial codes generation, theme search, theme review, definition, and naming, report production. NVivo Version 12 was utilized in coding and it helped to organize, retrieve and compare the data coded systematically across the interview corpus. The first round of coding was inductive whereby the themes were revealed naturally out of the data and then a deductive layer of coding was put in place to help in linking emergent themes with the existing doctrinal and theoretical literature.

The use of various complementary strategies helped to establish rigor and trustworthiness. The combination of the interview with the data of the doctrinal legal analysis and secondary sources made methodological triangulation possible. Member checking was done through the sharing of summary of interviews with participants so that they can have a chance to verify and correct any errors. The peer debriefing consisted of a routine conversation about the findings that emerged with a colleague who was a sociolegal researcher. The entire audit trail was kept of all methodological decisions, analytic procedures, and interpretive choices that allows an independent assessment of the research process. Reflexivity of the researcher was anticipated in the entire study, and the researcher critically evaluated his/her positioning as a legally trained researcher who had prior ideas on the provisions of the PECA.

Ethical Considerations

The Institutional Review Board of the university gave ethical consent to the study before data collection. The entire participation was voluntary and informed consent was taken in writing by every participant before he was interviewed. The participants had been given an information sheet in plain language that spelled out the purpose of the study, the type of involvement that they were going to have, that they could leave the study at any point in time without repercussions and that they were assured of their confidentiality and anonymity. Transcripts were stripped of all identifying information and all research products used pseudonyms in place of the actual names of participants. The audio records were stored in a password-protected encrypted server that could be accessed by the main researcher and were deleted at the end of the research.

Findings and Analysis

Theme 1: Evidentiary Dilemmas and Digital Forensic Inadequacies

The most widespread and most frequently mentioned issue across the categories of participants was the issues related to the digital evidence, its gathering, retention, validation, and admissibility in cybercrime trials. Respondents spoke of a systemic lack of forensic capability that they believed to be the greatest consequence of successful prosecution of cybercrime via PECA. A veteran attorney in criminal law has referred to the apparent state of evidence in cybercrime cases as inherently asymmetrical, where the prosecution has to prove beyond any reasonable doubt that someone is guilty, but the evidence provided to support the chain of digital evidence is often insufficient to support it to the required standard to make the findings stand in court.

Judges sampled in the research had major concerns related to the quality of the digital evidence that is regularly produced in cybercrime cases. Based on PECA case adjudication by a judge in a six-year-old cybercrime court, in most of the trials in dispute, the integrity of the chain of custody, the effectiveness of the forensic tools to extract and analyze data, as well as the credentials of prosecution witnesses testifying as the expert in the field of digital forensics, were challenged by the defence counsel. The judge noted that in a number of cases, where there was no proper authentication documentation, the resulting consequence was the exclusion of otherwise probative digital evidence with resulting consequences on prosecution results.

This image was supported by the investigators of FIA on the functional level, and was found to have three direct forensic weaknesses, which they termed systemic: a lack of hardware and licensed forensic software tools in regional NR3C offices outside Islamabad; a lack of trained digital forensics staff in relation to cases; and a lack of a standardized forensic protocol that dictates the seizure, imaging and analysis of digital One of the investigators observed that most of the devices that appeared before the analysts in the field of forensics are not immediately separated off the networks after seizure and this may be affecting the integrity of volatile data. This finding is in line with what Hussain and Bashir (2021) found as the main source of evidentiary vulnerability in cybercrime in Pakistan: poor seizure procedures.

The overlap between this manner of finding difficulties with the evidentiary issues and the specialized demands of the PECA authentication features proved to be a theme of trouble to the legal community. The PECA section 41 is that the electronic evidence must also have a certificate of a responsible official of the owner of the device or any other person who has a lawful control of the device which certifies that the evidence is intact. According to the participants, this prerequisite, based on the

requirements in the English and the Indian law, is often difficult to fulfil in the situations when the digital evidence has been obtained by third-party providers, foreign servers, or devices that are owned by suspected criminals- in the latter case; an independent certifying official cannot be easily identified. As some of the lawyers mentioned, they had won their cases on this very reason, even though they thought that the piece of digital evidence in question was very real and incriminating.

Theme 2: Legislative Pasteboards and Definitional Cronies

The second significant theme that was revealed by the data was the definitional ambiguities inherent in the statutory language of PECA that respondents in all groups reported to create a high amount of interpretive challenge and legal uncertainty. The most commonly mentioned ambiguity was the one relating to the speech-related offences in the Act with the focus on such provisions as 10A, 20, and 37. The participants said that these provisions were characterised by conceptual imprecision that made it hard to be certain whether specific conduct fell within or outside the statutory prohibition, leading to under-enforcement, in which prosecutors chose not to prosecute because they were unsure about whether the specific conduct was within or outside the coverage of the statutory prohibition, and over-enforcement, in which prosecutors prosecute conduct that was outside.

The academics of law interviewed as part of the research presented the critical doctrinal assessment of the PECA definitional framework. A constitutional and information technology law scholar suggested that the definition of the term information system in Section 2(1)(n) was generally broad enough to encompass most of the digital technologies of the era, but lacked specificity enough to be useful in situations where new forms of technological architecture such as blockchain networks, decentralized applications, and Internet of Things devices were involved. According to the scholar, various prosecutions had been postponed or rejected on the basis that the parties could not reach an agreement as to whether the system allegedly accessed or otherwise interfered with met the statutory definition, and that no reported judgment had yet answered this question conclusively.

Special critical attention was given to the crime of cyberterrorism stated in Section 10A. The respondents reported that the definition of cyberterrorism in the provision is incredibly broad and embraces any use of an information system that is likely to produce fear or insecurity in any population or is intended to damage the cohesion, integrity, security, or sovereignty of Pakistan, which participants claimed was vulnerable to being politicized. An experienced criminal lawyer who has defended cases brought under Section 10A explained some instances where the Section 10A was used to prosecute political activists and journalists whose publications posted online were alleged to pose a threat to national security, and had no material connection to terrorism as the term is commonly understood. The trend coincides with the anxieties reported by Human Rights Watch (2021) and Amnesty International (2022) about the abuse of the national security provisions of PECA regarding the civil society.

Judges observed that the ambiguity on the definition of PECA posed both a problem on sentencing and on determining the liability. The lack of sentencing principles, which were particular to the offences of PECA, implied that the sentencing in cybercrime cases was very diverse and uncertain, and the normative vacuum, which was created by the lack of laws, was occupied by the individual judicial discretion. A judge noted that this uncertainty had an important bearing on the deterrence role of punishing cybercrime, which negated the preventive effects of the Act. Similar claims have been voiced by Shah and Afridi (2020) regarding sentencing inconsistency in Pakistani cybercriminal courts, which the authors have described as a systemic phenomenon associated with the application of PECA, which requires an immediate legislative response.

Theme 3: Complicated Jurisdiction and Implementation Restraints

Jurisdictional complexity was a third important thematic cluster, with participants citing internal jurisdictional complexity, which occurred due to the constitutional segregation of powers between federal and provincial governments in Pakistan as well as external jurisdictional complexity which occurred because of transnational nature of most cybercrime crimes. PECA makes cybercrime a federal topic under FIA investigation, yet those involved reported that a grey area between cybercrime and provincial criminal law, terrorism law and civil proceedings produced an entirely confusing and occasionally conflicting jurisdictional environment that might cripple investigations and thwart prosecution.

The challenges of developing cases against the suspected offenders who moved outside Pakistan were characterised with urgency by investigators and lawyers. Most of the cybercrime crimes involving victims or institutions in Pakistan were said to through foreign locations but the ability to retrieve digital data on foreign servers, suspects using virtual private networks or performing investigative mandates to foreign jurisdictions was said to be very poor in Pakistan. The key international legal framework to assist in cybercrime cases is the Budapest Convention and since Pakistan is not a signatory to the convention, bilateral arrangements to assist in cybercrime cases were described as ineffective, slow, and in practice not used.

In one case, according to the investigator, a large-scale financial fraud committed with the help of an online platform of a Pakistani bank was tracked to servers in three other countries, none of which had a mutual legal assistance treaty with Pakistan that would address the types of data that were being sought. The probe had been pending more than two years during which diplomatic avenues were pursued and by the time it was revived the evidence was thought to have been erased. The case presents an example of a structural weakness in the Pakistani architecture of enforcing cybercrime that PECA, with its domestic-oriented approach to investigative and prosecutorial schemes, fails to account for. Pakistan membership of the Budapest Convention or at least bilateral agreements with key data-giving jurisdictions were requested by a number of participants as a priority reform.

Theme 4: Tensions of due process and basic rights concerns

The fourth conceptual area included the reflections of the participants concerning the conflict between a successful cybercrime prosecution and the constitutional rights of the accused individuals and third parties. This conflict was felt most intensely in three areas the scope of the search and seizure authority of PECA; the terms of pretrial detention and bail; and the interplay between the content-related measures in PECA and the constitutional right to freedom of expression contained in Article 19.

Defense counsel representing defendants in PECA explained the investigative authority granted to the FIA in the section 29 to 38 of the Act as extraordinary by nature as it authorizes the search and seizure of any information system, device, or data without a warrant in instances where the investigating officer had a reasonable reason to suspect that a PECA offence was being executed. Though the Act demands ex post facto judicial sanction of such seizures within twenty-four hours, respondents noted that judicial restraint was often formal and superficial as opposed to being substantive. Clients had their whole digital lives stolen, including personal communications, financial data, work emails, and so on, and had been retained without a judicial review of the reasonableness of any of it.

Another area of great due process concern was seen to be bail provisions under PECA. Some PECA crimes attract a maximum sentence of fourteen years, and thus they fall under the non-bailable offence category of the Code of Criminal Procedure, meaning that suspected criminals often served lengthy pretrial detentions as their cases were processed in the already overloaded cybercrime courts. One judge admitted that the duration between the charge and the final judgment in the cases of cybercrime that appeared before their court averaged two to three years, a time frame that exerted great hardships on persons who were found not guilty.

Theme 5: Constraints of Institutional Capacity

The last and fifth thematic area touched on the larger institutional framework in which PECA prosecution occurs with the players attributing serious capacity limitations in various aspects of the criminal justice system. The participants also indicated that training and knowledge in digital technology among the judicial officers are a major deficit in all the professional categories. One legal scholar noted that PECA created special courts to deal with cybercrimes, but failed to ensure that the judges who took up their appointments had any technical qualification in digital technology or special training in legal and technical aspects of cybercrime. What ensued was a judiciary that was supposed to determine extremely technical questions of evidentiary and legal nature without proper preparation.

The prosecutors in the FIA were also reportedly working with the conditions of chronic under-resourcing. According to the participants, the NR3C, which investigates cybercrime at the national level, was working with a small portion of the human resources that other similar jurisdictions used in investigating cybercrime and that staff turnover was high due to the fact that the private sector offered better remuneration than the NR3C and as a result; institutional knowledge was being drained regularly. A researcher approximated that the median NR3C officer only spent less than eighteen months of field training in digital forensics, not enough time to become knowledgeable enough to conduct intricate cybercrime investigations.

Providing legal assistance to defendants in cybercrimes was also found to be another system failure. Numerous defendants especially in the lower socioeconomic groups did not have the means to hire attorney services of cybercriminal knowledge, and the legal aid system was unavailable to such specialized services. Inequality of arms at the time of cybercrime proceedings was reported by some of the participants as being incompatible in the essence with the right to a fair trial under the Article 10A of the Constitution. This finding aligns with the wider body of access to justice research of criminal courts in Pakistan and demonstrates the systemic nature of issues that face prosecution of cybercrimes..

Discussion

The effects of this studies exhibit a regular and rather demanding photograph of what cybercrime prosecution need to do regarding PECA 2016 in Pakistan. When combined, the 5 recognized classes of thematic problems, i.e., evidences of

insufficiency, uncertainty in definitions, criminal and jurisdictional complexity, anxiety and problems of due technique, and constraints of institutional potential may be visible as an interdependent device of issues that can not be resolved individually. Unless an answer is given to the alternative dimensions of the problem, it's far anticipated that redressing any of them will now no longer have a widespread impact on enhancing the exceptional and effectiveness of cybercrime prosecution.

The recognized problems in evidentiary demanding situations related to the existing observe may be traced to the broader frame of global literature on the subject of virtual forensics and the regulation of virtual proof (Casey, 2011; Mason and Seng, 2017), however are heightened withinside the state of affairs of Pakistan because of the particular institutional shortcomings of the NR3C and the shortage of internationalized forensic techniques. Perhaps the maximum short-time period consequential difficulty is the discrepancy among the extent of proof that an powerful prosecution may be added towards an character beneathneath PECA, on one hand, and the forensic potential this is frequently reachable to investigators, on the opposite, due to the fact that this at once and quantitatively influences the end result of prosecutions. To take away this hole it's miles vital to put money into forensic infrastructure and employees improvement and standardization of protocols which, however, have to be followed via way of means of legislative causes of the authentication of virtual proof.

The ambiguities in definition recognized on this paper resonate with the prevailing concerns approximately the enforcement of cybercrime rules in different growing countries (Chawki et al., 2015; Ibrahim, 2016), but it appears in particular applicable to the scenario in Pakistan because of the mounted tune document of PECA software in competition to political opponents, journalists, and civil society (Human Rights Watch, 2021). The normative war among powerful cybercrime prosecution and a loose expression safety isn't always some thing extraordinary to Pakistan--a in addition aggravating stability has been struck withinside the enactment of cybercrime law via way of means of jurisdiction, however PECA has been inclined to move too some distance in its contemporary-day draft because of the effect of enforcement on the fee of rights safety. There is an pressing want to enact legislative reform primarily based totally at the ideas of proportionality defined withinside the charter jurisprudence of Pakistani charter.

The jurisdictional and worldwide cooperation problems determined withinside the present day paper suggest the relative isolation of Pakistan withinside the international framework of cybercrime enforcement cooperation. The truth that the usa of Pakistan has now no longer been the signatory to the Budapest Convention denies the investigators on this u . s . a . get entry to to the community of mutual prison help approaches and to the harmonized evidentiary requirements that the Convention offers, with a view to now no longer be addressed truly with the aid of using nearby legislative reform. Participation withinside the global cybercrime regulation governance forums, inclusive of the present day negotiations of a brand new United Nations cybercrime convention, is every other vast complementary factor of reform.

Conclusion

This paper has added a holistic qualitative file at the troubles of regulation dealing with prosecution of cybercrime in PECA 2016 in Pakistan primarily based totally on each the doctrinal and empirical interview proof, and the effects are analytically sound and nearly applicable. The 5 styles of recognized thematic demanding situations, particularly the shortage of proof, polysemy, jurisdictional complexity, anxiety on due method, and absence of institutional potential, reveal a criminal framework that, although it has legislative ambitions, leaves a good deal to be favored in phrases of supplying an powerful and rights-respecting framework thru which cybercrime is prosecuted withinside the contemporary-day virtual putting of Pakistan. These outcomes endure a long way-attaining implications on regulation practitioners, judicial officials, policymakers and educational students investigating the contemporary-day components of the cybercrime regulation of Pakistan.

Recommendations

The maximum essential and a long way-achieving idea that arises out of this take a look at is the legislative reform of PECA 2016. The definitional provisions of Section 10A, 20 and 37 ought to be amended so that you can deliver in greater precision and proportionality, clean definition of key phrases, express list of the harms geared toward and stringent treatments in opposition to misuse to serve political or different malicious purposes. Section forty one on authentication necessities of virtual proof ought to be amended to provide possible steerage of instances in which proof is retrieved primarily based totally on third-birthday birthday celebration offerings and overseas servers. The sentencing rules on PECA offences are to be formulated and issued that allows you to reduce the inconsistency and the uncertainty that prevails in sentencing cybercrime offenders.

Digital forensic potential desires institutional funding. Significant growth of the NR3C is needed in the quantity of employees and technological infrastructure, in which precise forensic laboratories are created withinside the capital of every province with present day forensic system and authorized software. All FIA investigators coping with cybercrime instances have to be

added to obligatory standardized education in virtual proof series and maintenance tactics, and a pro improvement tune that guarantees ongoing improvement in virtual forensics experts needs to be created to cope with the continual difficulty of professional attrition.

They need to recruit judicial officials to paintings withinside the courts of cybercrime through obligatory specialised schooling on each the technical elements of virtual proof and the felony specificities of PECA. The improvement of this schooling must be completed along side generation experts, regulation professors, and non-governmental companions which have enjoy in schooling approximately cybercrime. Judicial schooling curriculum have to be often reviewed and modified to in shape the development withinside the virtual era, in addition to the converting traits of cybercrime.

Pakistan should searching for to enroll in the Council of Europe Convention on Cybercrime (Budapest) in order to permit it to get right of entry to an already advanced machine of mutual felony help and worldwide cooperation regarding cybercrime research. Certainly, withinside the meantime, bilateral agreements with principal jurisdictions containing information have to be negotiated to confront the feasibility limitations of obtaining proof saved on overseas servers. Pakistan need to additionally undoubtedly take part withinside the United Nations method of formulating a brand new worldwide cybercrime convention.

Lastly, there's the crucial size of PECA implementation at the component of essential rights, with a view to ought to be addressed immediately. A separate manipulate mechanism desires to be created a good way to oversee the exercising of research powers with the aid of using PECA, developments in prosecution, and post to the overall public on opportunities of abuse. There have to additionally be an stronger provision of prison useful resource to defendants in cybercrime instances so that you can make certain that the accused people have get right of entry to to suggest with the applicable expertise, and the bail regime of PECA offences have to be revisited to make sure that the duration of the pretrial detention ought to be proportional and the detention of the accused humans who turn out to be acquitted ought to be saved as a minimum.

References

1. Ali, Z. (2022). Free speech versus cybercrime control: Constitutional analysis of PECA 2016's speech offences. Pakistan Law Review, 14(2), 45–78.
2. Amnesty International. (2022). Pakistan: PECA used to silence journalists and activists. https://www.amnesty.org/en/documents/asa33/5461/2022/en/
3. Banakar, R., & Travers, M. (Eds.). (2013). Law and social theory (2nd ed.). Hart Publishing.
4. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa
5. Braun, V., & Clarke, V. (2022). Thematic analysis: A practical guide. SAGE Publications.
6. Brenner, S. W. (2010). Cybercrime: Criminal threats from cyberspace. ABC-CLIO.
7. Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers and the internet (3rd ed.). Academic Press.
8. Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. (2015). Cybercrime, digital forensics and jurisdiction. Springer.
9. Clough, J. (2015). Principles of cybercrime (2nd ed.). Cambridge University Press. https://doi.org/10.1017/CBO9781139540612
10. Council of Europe. (2001). Convention on cybercrime (ETS No. 185). Council of Europe Treaty Office. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
11. Daskal, J. (2018). Borders and bits. Vanderbilt Law Review, 71(1), 179–240.
12. Human Rights Watch. (2021). Pakistan: Cybercrime law used to silence critics. https://www.hrw.org/news/2021/05/26/pakistan-cybercrime-law-used-silence-critics
13. Hussain, Z., & Bashir, S. (2021). Digital forensic capacity in Pakistan: An assessment of FIA's NR3C. Journal of Law and Technology in Pakistan, 3(1), 22–45.
14. Ibrahim, S. (2016). Cybercrime in developing economies: Challenges and responses. Computer Law and Security Review, 32(6), 890–906. https://doi.org/10.1016/j.clsr.2016.07.007
15. Mason, S., & Seng, D. (Eds.). (2017). Electronic evidence (4th ed.). Institute of Advanced Legal Studies for SAS Humanities Digital Library.
16. Mustafa, U. (2021). Anatomy of ambiguity: Legislative drafting deficiencies in the Prevention of Electronic Crimes Act 2016. Islamabad Law Review, 5(1), 1–34.
17. Prevention of Electronic Crimes Act, No. XL of 2016 (Pakistan). https://www.na.gov.pk/uploads/documents/1474888191_266.pdf
18. Rahman, A. (2022). Five years of PECA: Assessing implementation outcomes and reform imperatives. Pakistan Journal of Criminology, 14(2), 88–116.
19. Selwyn, N. (2016). Is technology good for education? Polity Press.

20. Shah, F., & Afridi, M. (2020). Admissibility of digital evidence under PECA 2016 and Qanun-e-Shahadat: An analytical study. Journal of Law and Society, 51(2), 178–203.
21. Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Polity Press.
22. Waseem, Z. (2017). Prosecuting cybercrime in Pakistan: Early reflections on PECA 2016. South Asian Journal of Law and Policy, 2(1), 56–82.