The Journal of Arts, Sociology and Humanities

JASH, Vol. 4 No. 1 (2026). Homepage: https://thejash.org.pk/index.php/jash

Cyber Legislation in Pakistan: A Critical Analysis of Legal Frameworks for Electronic Transactions, Cybercrimes, and Digital Evidence

Mahboob Usman[1] and Zeeshan Ashraf[2]

[1]The Ministry of Religious Affairs and Interfaith Harmony, Islamabad. *The opinion expressed in this article is solely of the author and has no nexus with the Ministry*. Email: mehboob_usman@yahoo.com

[2]Head of Department, IVY School of Law, Lahore

Abstract

Information and Communication Technology (ICT) has revolutionized everything by causing a paradigm shift from centuries-old practices to the digital revolution. This revolution has also affected the legal system of the world, including Pakistan. Laws on criminal and civil procedures were enacted long before the appearance of information technologies, when nobody had any idea about the computer and the internet. Thus, this development also changed the nature of evidence worldwide and has expanded significantly in the modern digital era. A lot of data is created in digital form, and most of the data and information is never printed. The laws made prior to the invention of the computer and the internet were meant for an ordinary environment and were not compatible with the cyber environment. Various attempts were made in Pakistan to cover the existing lacunas at the time and provide a mechanism for dealing with the latest developments in the field of information technology. On coming to know the issues faced by the Pakistani society, the legislature enacted new laws to provide a remedy to the people and provide a proper forum for redressal of their grievances. This paper attempts to analyze the extent to which Pakistan's legal reforms concerning digital evidence and information technology have effectively addressed the challenges arising from the cyber environment, and whether these reforms are sufficient to provide comprehensive legal protection and remedies for affected individuals.

Keywords: Cyber Laws; Cyber Security; Law of Evidence; Digital Evidence; ICT

Introduction

After the independence, the government of Pakistan adopted all the existing laws, which are still in force with some modifications (Usman, 2022). In the 1980s, Information Communication Technology started emerging, enabling the legislature to legislate on new aspects of technology, such as the Electronic Transactions Ordinance (ETO) and Prevention of Electronic Crimes Act (PECA), which were enacted, besides amending certain provisions of the law of evidence. Whenever any attempt was made to change the existing law related to cyberspace, many people started criticizing the government, saying that the government is restricting the freedom of expression granted by the Constitution of Pakistan, and on the other side, the government says it protects the rights of individuals granted under the law of the land. Whether these laws are beneficial for the Pakistani society or instead of blessing these laws making difficulties for the common people of Pakistan? This aspect will be analyzed in this article.

The Indian Evidence Act 1872 was passed by the Imperial Legislative Council in 1872, and the same came into force on 1st September 1872.

Nevertheless, since its enactment, without changing its original form, a few amendments were made in it; however, this law was repealed through the Qanun-e-Shahadat Order 1984. The term "Qanun-e-Shahadat" is only an Urdu translation of the English term "Law of Evidence is the basic legal instrument on law of evidence in Pakistan; the aim of this law is to bring the existing law of evidence in conformity with the injunctions of Islam (Carroll, 2006). In fact, all the Articles 3, 4-6, 42, and 44 of QSO are substantially and subjectively mere reproductions of all sections of the repealed Act with few exceptions. However, Article 1 (2) of this law does not apply in arbitration proceedings.

Notwithstanding, the most significant development of the QSO was Article 164, which provided for the admissibility of modern devices, which reads as "[i]n such cases as the Court may consider appropriate, the Court may allow to be produced any evidence that may have become available because of modern devices or techniques." It was the beginning of Information Technology (IT), when the existing law of evidence was changed through QSO, making it difficult to predict future issues covering emerging technologies. However, the 164 Article was not sufficient to address IT-related issues comprehensively and provide a proper mechanism for electronic evidence. Yet, it provided recognition and acceptance of the new devices in evidence. But with the passage of time, it failed to fulfill legal requirements; therefore, the legal fraternity criticized the opinion of Muhammad Aqil, ASC, who expressed grave concerns. He further stated that this order was promulgated "as a tool for denial of justice to private parties by providing legality to conversations in private/personal disputes of civil and commercial nature as evidence in courts."

Besides, criticizing the QSO he stressed that in modern technological and computer age, "it has become far more easier to fake up evidence by using, erasing, tampering and making interpolations in audio/video cassettes/CDs and preparing fake and fabricated tapes/cassettes/CDs and morphed up images by parties trying to establish false, fake and fabricated claims against rivals in all types of litigations, be it civil, commercial or criminal." That "even the government and the politicians have felt the brunt of this Article…as with the help of mimickers, camera-tricks and various electronic devices and techniques, including computer soft-wares blackmailing, false, fabricated and frivolous claims have been made by vested interests to exploit and use against adversaries in courts." Further, he feared that "such dirty tricks not only destabilizes the social structure of a society but also promotes immorality, extortion, terrorization, scandalization, forced marriages and sometimes sensationalization of issues." and emphasized for amendment of this article to avoid its misuse and to bring it with the contemporary requirements of the legal system of Pakistan.

A "National Conference on Law and Technology in the Digital Age" was organized by the civil society in 2017 at Islamabad in which various speakers including Hildy Bowbeer (from USA), Muhammad Amir Munir from PJA, Justice (R) Tassaduq Hussain Jillani, Justice (R) Shakirullah Jan, Dr. Tariq Hassan, ASC and Muhammad Aqil, ASC expressed grave concerns "over misuse of modern devices and techniques for ulterior motives, illegal & wrongful gains and called for repealing" (Dawn, 2018) of Article 164. While criticizing the QSO, they said that "gross injustices existing in the society along with evils of harassment, blackmailing, and frivolous litigations based on evidence procured through illegal use of modern devices and techniques for ulterior motives, illegal and wrongful gains" is not sustainable, which needs to be addressed by the legislators.

They demanded a "fair and just law of evidence as the need of the hour" (Dawn, 2018). Justice Tassaduq Hussain Jillani (retd) said the gap between technological innovation and the legal rules necessary to govern such developments is ever-widening. It is a must to develop and pursue rational, efficient policies in order to ensure that Pakistan makes the best possible use of technology as a

driving and democratizing force, accommodating business and entrepreneurs, while protecting the rights and the privacy of the consumers and the public at large. Keeping this in view, regulation must ensure that the internet and the world of technology are a safe and equitable place.

Similarly, another seminar was organized in the same year by the RAC in collaboration with IHRA to create awareness of the flaws in the law of evidence of 1984, in which members of the civil society requested the Supreme Court of Pakistan to take notice of the misuse of QSO. In the RAC seminar, Mian Javed Anwar Advocate observed that "the faulty Articles 46-A & 164 of Qanoon-e-Shahadat' Order, 1984 should be a matter of immediate attention of the top judiciary, keeping in view that the flaws in these articles are grossly being misused." Some people think that the tape-recorded conversations should not be made admissible in the law of evidence. One of the critics is Syed Ghulam Raza Shah Naqvi, who explained this phenomenon in the above-mentioned seminar of RAC and said that "the tape-recorded conversations inclusive of privileged relating to private, personal matters such as between the husband-wife, lawyer-client, doctor-patient or relatives, etc., should not be made admissible under the law of evidence (Dawn, 2018). However, instead of amending Article 164 of the QSO, a proviso with the following words was added: "Provided that conviction on the basis of modern devices or techniques may be lawful."

In the early days of the 80s, the legislature could hardly have foreseen the future of digital evidence, including the storage of vast volumes of data by organizations on the internet, and storage of data beyond national boundaries, such as cloud systems, which are providing cross-border services to many companies around the globe. Now, after four decades of insertion of Article 164 in the QSO, and after two decades of amendment of Article 2 in the QSO (as amended through ETO in 2002), the need to "accord with changing technology" is not fulfilled yet. Existing rules of evidence, being centuries-old, were still being applied to digital evidence; therefore, the question arises whether the current evidence rules recognize the unique nature of digital evidence. As electronically stored information (ESI), such as embedded data, web caches, browsing history, temporary history, cookies, and backup files, is not addressed in the QSO. Article 164 of the QSO was unable to provide a comprehensive mechanism for the consideration of each type of digital world issues. Therefore, this article was amended in 2023 as under: 164. Production of evidence that has become available because of modern devices or information systems, etc. Depending on the nature of the case and circumstances, the court may, if it deems appropriate, allow to be produced any evidence or witnesses recorded by the court through modern devices or techniques, including video call, Viber, Skype, imo, WhatsApp, Facebook Messenger, line caller, and video conference, etc. (Criminal Laws (Amendment) Act 2023).

Deriving wisdom from this article, the legislature in Pakistan provided that the examination of rape victims and witnesses can be recorded by using video-link under Section 7 of the Anti-Rape (Trial Procedure) Rules, 2022, and under Section 9 of these rules, evidence can also be recorded through video conferencing. Since technology is growing at a fast rate, it is making it hard for contemporary systems to cope with advancements in technological devices; thus, the requirement for admission of this type of evidence is also changing. Would an electronic record constitute a document Article 2 (1) e of the QSO? Are the contents of Article 78-A of QSO electronic records writings? Can Article 73 of QSO electronic records be accepted as evidence? These are the few issues addressed by the amendments in QSO through the enactment of ETO.

Article 2 of the QSO was amended, and two new sub-clauses, namely (e) and (f), were added, and various expressions were defined, such as automated, electronic, information, information system, electronic document, electronic signature, advanced electronic signature, security procedure, and certificate, which opened a new era for electronic transactions. Moreover, Articles 30, 59, 85, and

Article 73 of QSO were amended, while new Articles 46-A and 78-A were also inserted in it. The question arises whether these modifications are applicable to all proceedings, either civil, criminal, or commercial, or to the selected laws? Stating differently, whether this amendment is ETO specific, or has amended the QSO? However, section 29 of the Ordinance speaks otherwise.

Research Methodology

The methodology of this research is based upon multiple approaches of legal scholarship, including a comparative law approach and case laws. Moreover, a major portion of this research is based on library research that references are in the form of books, Statutes, Articles, Reports, and decided cases of the superior courts of Pakistan. Moreover, cyber legislation, both in civil and criminal matters, will be discussed.

Discussion

1. Electronic Transactions Laws

Despite the fast advancement of information technology, electronic transactions are growing gradually in the world. Keeping in view the requirement of international business-related transactions, the Electronic Transactions Ordinance (ETO) was promulgated in 2002 to provide for "recognition and facilitation of documents, records, information, communications and transactions in electronic form, accreditation of certification service providers." It also paved the way for the criminalization of certain cybercrimes prevailing (or known) at the time. Besides, through the promulgation of this ordinance, computer-generated documents were given legal recognition. Section 3 of ETO says that "[n]o document, record, information, communication or transaction shall be denied legal recognition, admissibility, effect, validity, proof or enforceability on the ground that it is in electronic form and has not been attested by any witness." Before the promulgation of ETO, it was mandatory for documents to be in written form, but the same was dispensed by the ETO. Similarly, Sections 5 & 6 of the ETO waived the requirement of original form, and data retention was also waived when the original was in electronic form. Moreover, Section 7 of the ETO says that where signatures were required on the documents, electronic signatures were recognized. Now, Section 9 is a presumption of authenticity, and integrity is attached to the electronic signature. Nonetheless, Section 8 of the ETO electronic signatures can be verified, as per law, in any manner, to verify their authenticity and integrity.

Under the Stamp Act 1899, stamp duty was imposed on legal instruments, but Section 10 of the ETO has removed this condition on electronic instruments until the finalization of appropriate measures by the government. On the one hand, Section 10 and 11 of the ETO suggest the conditions for notarization and attestation of documents was removed till determination of final measures for attestation and notarization, and Section 13-15 of the Act on the hand procedure for attribution of communications and acknowledgment of electronic receipt was also provided in ETO. However, Section 16 of the ETO does not confer any right upon any authority to accept, issue, create, or preserve any document in electronic form.

The main function of this ordinance is the establishment of the Electronic Certification Accreditation Council, which is, inter alia, exclusively under Sections 21 and 22 of the ETO, responsible for "granting and renewing accreditation certificates to certification service providers," monitoring the accredited certification service providers, establishing and managing the repository, and conducting research in cryptography services. Section 24 of the ETO states that the Certification Council is exclusively responsible for granting accreditation to certification service providers and for other allied matters. Earlier, the use of cryptography was not allowed under Section 57 (2) (ah) of the Pakistan Telecommunication (Re-

Organization) Act, 1996. This ordinance also removed the restriction imposed on the use of cryptography. An accreditation certificate is mandatory for certification service providers. All certificates issued by the accredited certification service providers are managed by a repository established by the Certification Council.

Unlike Section 197 of the Pakistan Penal Code, issuance of a false certificate by the certification service provider was prescribed as an offense under Sections 34 and 35 of ETO, and provision of false information by the subscriber was also made an offense. Section 36 of the ETO Violation of privacy of information was made an offense punishable with imprisonment and fine. Moreover, Section 37 of the ETO states that there was a perception that someone may damage the information system; thus, this was also criminalized, and punishment was prescribed in this ordinance. But, sections related to the violation of privacy of information and damage to information systems remained in the field till the enactment of PECA in 2016, when these sections were omitted from the ETO.

Section 30 of this ordinance was given overriding effect, and words assuming a paper tangible medium were extended to electronic forms. However, Section 31 is negotiable instruments, power-of-attorney, trust, will, and contract of sale were excluded from the preview of this ordinance. Besides, the provisions of this ordinance were extended outside Pakistan under Section 32. In light of the preamble and Sections 36 and 37 of ETO, it can safely be concluded that this instrument only covers a limited area of information technology-related issues. LEA's personnel, without bothering its true spirit, were using two sections of this ordinance to apply in every cybercrime situation, but the same were not fulfilling the requirements of prevailing circumstances; thus, these sections were amended by PECA.

ETO enabled a mechanism for electronic transactions, the Payment Systems and Electronic Fund Transfers Act (PSEFTA), provide a way forward "to supervise and regulate Payment Systems and Electronic Fund Transfers in Pakistan and to provide standards for protection of the consumer and to determine respective rights and liabilities of the financial institutions and other Service Providers, their consumers and participants" (The Payment Systems and Electronic Fund Transfers Act, 2007). Thus, it is obvious from the preamble of this Act that this Act provides a regulatory framework for payment systems and electronic fund transfers. Under Sections 3-4 and 12-14 of PSEFTA, it opened a system for electronic funds transfer, which was not available before it. Inter alia, it provided for the powers of the state bank in respect of the designation and revocation of the payment system and Real Time Gross Settlement (RTGS) System. Besides, it also provided for the designation, issuing, and prohibition of payment instruments, provisions for clearing houses and their obligations, supervisory control of state banks, documents of transfers, notification of error, liability of parties, and proceedings before the court. No doubt, this legislation is a blessing for e-commerce in Pakistan. Had this not been done, Pakistan would have been behind in the development of e-commerce. In Pakistan, for a long time, tax was not being imposed on digital proceeds; now the same has been brought into the tax net through the recent enactment of law on the subject (Digital Presence Proceeds Tax Act, 2025).

For simplifying the cross-border trade process and reducing the cost of doing business in Pakistan, the GoP has established the Pakistan single window (Pakistan Single Window Act, 2021), which provides for managing the country's external trade. Without promoting investment in technology, it will not be possible to promote e-commerce and e-governance in the country, therefore, special technology zones have been established for the development of "scientific and technological ecosystem" (Special Technology Zones Authority Act, 2021) In line with the vision and policy of GoP, it has also introduced e-governance system for its departments and established a Board for e-governance (National Information Technology Board, 2022).

Initially, the Government of Pakistan (GoP) prepared the Digital Pakistan Policy (Islamabad: M/o IT & Telecom, 2018) to provide a digital ecosystem. Later, this policy was transformed into the enactment of the Digital Nation Pakistan Act, 2025, for "transformation of Pakistan into a digital nation, enabling a digital society, digital economy and digital governance." Similarly, the GoP, realizing its vision for a digital nation, has also framed the National Artificial Intelligence Policy for ethical and responsible use of AI technologies. Moreover, GoP has provided legislation for transactions in virtual assets (Virtual Assets Ordinance, 2025).

2. Prevention of Electronic Crimes Laws

ETO amended Article 2 (1) sub clauses (e) and (f) of the QSO, defined some expressions, added a few new Articles 46-A and 78-A, and added some explanations in the existing Articles 30 and 73 of QSO, which was an upright step towards the legislation on cyber-related issues. Thus, it can be said that this ordinance provided a legal system for the recognition of electronic records rather than penalizing the criminals; therefore, it was not sufficient to tackle the cybercrimes prevailing at that time. Whenever any issue was brought to the knowledge of LEAs, due to a lack of proper legislation on the subject, they used to apply sections 36 and 37 of ETO. Resultantly, the accused were acquitted of the charges, due to improper application of the law. Keeping in view this situation, a need for a comprehensive law on the subject was felt, which led to the promulgation of the Prevention of Electronic Crimes Ordinance, 2007.

The Prevention of Electronic Crimes Ordinance 2007 was promulgated to raise awareness of electronic crimes. This ordinance was not tabled in the parliament and lapsed after completing its constitutional life. Consequently, this ordinance was again promulgated in May 2008 and later in February 2009; the last promulgation took place on 4th July 2009. In Pakistan, the Presidential Ordinance is applicable for one hundred and twenty days from the date of its promulgation. Therefore, Pakistan, for a long time, remained without a cyber prevention law (Pro Pakistan, 2014).

In 2016, the parliament enacted the Prevention of Electronic Crimes Act (PECA, 2016), which provided provisions for the prevention of electronic crimes. Stating differently, it is an Act which makes provisions to "prevent unauthorized acts with respect to information systems and provide for related offenses as well as mechanisms for their investigation, prosecution, trial and international cooperation."

Sections 3 to 19 of the PECA 2016 have penalized unauthorized access/copying and interference with information systems/data, including the unauthorized access and copying of critical infrastructure systems and data. Besides, cyber terrorism includes recruitment, funding, and planning of terrorism, hate speech, electronic fraud and forgery, malicious code, unauthorized use of identity information and issuance of SIM cards, unauthorized interception and tampering of communication equipment, and making, obtaining, or supplying devices for use in computer-related offenses. Even Sections 2 and 14 of the Protection of Pakistan Act 2014 on cybercrimes, if committed for waging war, are considered a separate category, and severe punishments are provided for committing this offense.

This Act has also established a specialized investigation agency to investigate cybercrimes (PECA Amendments 2025). Although the investigation agency, i.e., NCCIA under PECA, was a specialized agency for investigation of cybercrime, it lacks the capacity to examine forensic material; therefore, the GoP has established a National Forensics Agency under the National Forensics Agency Act, 2024. to "conduct examination of forensic materials and render opinion" whenever the same is required before the courts.

3. Blessings of PECA

Although PECA has criminalized many acts, whether the target of prevention of cybercrime is achieved, or is this Act being misused by the authorities? This needs to be examined in the light of court decisions. Rana Muhammad Arshad, a journalist by profession, was summoned by the FIA under the provisions of PECA through an undated and vaguely worded notice, without specifying the purpose of the summons. Feeling aggrieved by the said notice, he filled a Writ Petition 2939/2020 in the IHC challenging the vires of said notice, where, on the date of hearing the investigation officer of the FIA failed to satisfy the honorable court regarding commission of offence under the provision of PECA, therefore, the court observed that issuance of summon in hasty and recklessness had "obviously caused harassment and intimidation, not only to the petitioner but his family members as well" (Rana Muhammad Arshad v. Federation of Pakistan, 2021).

The court further held that "[t]he reckless action of the Agency in the case in hand is not an exception. This constitutional court has observed that either the provisions are being misinterpreted or they are being invoked in a reckless manner for other than germane considerations." Therefore, the IHC, considering the reckless and unprofessional manner of the FIA, inter alia, directed the D.G FIA to formulate guidelines for the investigating officers, besides it also directed the Federal Government to take "prompt and effective action to prevent the abuse of coercive powers under the PECA."

Section 37 of the PECA has authorized the removal of online unlawful content and unlawful and offensive online content. The Ministry of Interior requested the PTA to block Virtual Private Networks (VPN), but later these instructions were withdrawn as they were not in accordance with the law (Dawn, 2024) because the law provides for the blocking of content, not tools.

Keeping in view the sensitive nature of cybercrimes, courts have directed that an inquiry is necessary before lodging an FIR (Meera Shafi v. Federation of Pakistan, 2022). Similarly, Social media protection tribunal, this is not new concept rather old one when this tribunal was established under PECOs, has been established to protect the rights of citizens. A person was accused of uploading photographs through a cell phone; however, he was granted bail (Fakhar Zaman v. State, 2021). Similarly, another person was accused of accusing the armed forces, and he was also granted bail (Muhammad Azam Khan Swati v. State, 2013). Had this not been taken into consideration by the courts, the accused would have remained behind bars.

Under Section 49 of the PECA, the constitution of computer emergency response teams has been provided "to respond to any threat against or attack on any critical infrastructure information systems or critical infrastructure data, or widespread attack on information systems in Pakistan."

Petitioner was aggrieved of uploading of material on social media, and the FIA informed the court that he is unable to trace the source or ownership, therefore, the LHC considering it breach of privacy held that "Breach of privacy must be a felony… and making such material public should be intolerable by the state by invoking criminal laws as well as by society, by resorting to civil laws for damages". The High Court directed the authorities to make public the measures so taken, besides making it an official record (Hamna Qaiser v. Chairman PEMRA, 2024).

A Judicial Magistrate in Karachi, while hearing a case under PECA, said that social media posts pointing out the "lacunas and irregularities committed within the department" are healthy criticism (Dawn News, 2023). For sharing women's obscene videos on WhatsApp, a man was sentenced to nine years in prison (Dawn News, 2024). Similarly, in another case, a man was convicted of sharing his wife's explicit photos on WhatsApp (Dawn News, 2024). The LHC banned the cameraman from recording any person's video without their consent and considered it cyber-stalking (Vishal Ahmad Shakir v. Federation of Pakistan, W.P. No. 80758/2023). Now, the offenses mentioned in sections 21 and 22 of the PECA will be

investigated by the special sexual offenses investigation units (SSOIUs), Section 9 of the Anti-rape Act, not the investigation agency as prescribed in the PECA.

In a famous case (Rohan Ahmad v. the State, 2022), a case was registered against the petitioner under section 11 of the PECA, whereas the petitioner admitted the circulation of blasphemous material through WhatsApp; thus, his bail was rejected. In another case, the LHC also dismissed the bail application for sharing a banned translation of the Holy Quran through WhatsApp (Sheraz Ahmad v. the State, Crl. Rev. No.69407/2022).

The IHC granted bail for electronic forgery and fraud and imposed the condition of depositing money in the Trial Court for the grant of bail. Petition for leave to appeal was converted into an appeal, and the same was allowed by the SC, and the condition imposed by the High Court of depositing money in the trial Court was set aside, and the order of granting post-arrest bail was maintained (2023 SCMR 401).

4. Modesty of Natural Person and Minor

Section 20 (1) of the PECA says "Whoever intentionally and publicly exhibits or displays or transmits any information through any information system, which he knows to be false, and intimidates or harms the reputation or privacy of a natural person, shall be punished with imprisonment for a term which may extend to three years…" However, this section was amended in 2022, through Presidential Ordinance PECA 2022 and by this ordinance, the word "natural" was omitted and definition of person was changed which includes "any company, association or body of persons whether incorporated or not, institution, organization, authority or any other body established by the Government under any law or otherwise."

During an interview with Dawn News TV, Shireen Mazari claimed that some of the cabinet members in PTI's government objected/opposed to the PECA amendment Ordinance, 2022 (Dawn News, 2022). However, despite resistance from cabinet members, the ordinance was promulgated, which was later challenged in the IHC, and the court declared the ordinance in derogation of fundamental rights and, after declaring it unconstitutional, struck down the ordinance (Pakistan Federal Union of Journalists v. the President of Pakistan, W.P. No.666/2022).

Section 20 provides for the dignity of the natural person; however, this section was challenged in the LHC, alleging that this is against fundamental rights relating to freedom of speech guaranteed by Article 19 of the Constitution. However, the High Court held that this section is not unconstitutional, it is in conformity with the constitution. The LHC further held that this section is not discriminatory with sections 499 and 500 of PPC (Meera Shafi v. Federation of Pakistan, 2022).

In a landmark judgment (Irfan Sarwar v. the State, 2022), the IHC rejected the bail of the petitioner (for violating sections 20 and 22 of PECA) for creating fake social media accounts (Facebook and WhatsApp) and disseminating and uploading pornographic videos of children. Similarly, the IHC also dismissed the bail. Earlier, the Lahore High Court and Sindh High Court also rejected the bail. The vires of section 20 were challenged in the LHC, and the court declared that it is not ultra vires the constitution (Meera Shafi v. Federation of Pakistan, 2022).

5. Right to Fair Trial and Protection of Dignity

The Investigation for Fair Trial Act, 2013 (IFTA) provides for investigation for "collection of evidence by means of modern techniques and devices to prevent and effectively deal with scheduled offenses and to regulate the powers of the law enforcement and intelligence agencies and for matters connected therewith or ancillary thereto."

The purpose of this Act is obvious, as this Act is meant for the collection of evidence to the extent of the scheduled offenses which are mentioned in Schedule I of the Act. Evidence collected under this Act, Section 23 of this Act, to the extent of offenses

mentioned in Schedule I of the Act, is admissible, and the report of an expert is also admissible under this Act.

Section 38 of this Act has the overriding effect upon the QSO and CrPC. Thus, it is obvious that this Act is meant for specific offenses and a special treatment has been provided for the offenses under this Act, meaning thereby that it does not cover all aspects of digital evidence and related matters. In the USA, the Wiretap Statute prohibits the interception of oral, wire, and electronic communications. The same is prohibited in PECA and IFTA, respectively.

Nevertheless, speakers ignored the fact that the legislator had imposed certain restrictions on Law Enforcement Agencies (LEAs) for interception of digital data through the Investigation for Fair Trial Act, 2013 (IFTA).

In many security-related cases of Pakistan, surveillance or interception is used to trace the criminal under Section 3 (1) of IFTA. Before the enactment of IFTA, these powers were vested arbitrarily with the LEAs, but IFTA has provided a proper mechanism for the scheduled offenses.

Conclusion

Despite all public awareness campaigns by the government and banks, hackers are using more sophisticated techniques to breach the databases of banks and government institutions, resulting in depriving innocent people of their money and data, putting people at risk. However, the PECA has criminalized many digital crimes and provided relief to the people. When any issue was brought to the knowledge of the legislature, they enacted new laws to provide a remedy and a mechanism for redressal of their grievances. It is up to the people to follow the law and get benefits from this.

The amendment of the QSO to legislation on the prevention of cybercrimes and their investigation, along with the establishment of the national forensics agency, has paved the way forward for promoting the GoP idea for a digital nation. Had this initiative not been taken at the right time, we would have been far away from making policies on artificial intelligence and providing punishments for committing cybercrimes.

References

Carroll, L. (2006). Pakistan Evidence Order ("Qanun-i-Shahadat"), 1984: General Zia's anti-Islamisation coup. In M. K. Masud, R. Peters, & D. S. Powers (Eds.), *Dispensing justice in Islam: Qadis and their judgments* (p. 519). Brill.

Mason, S. (2007). *Electronic signatures in law*. Cambridge University Press.

Usman, M. (2022). Digital evidence: Testimony of expert witness in Pakistani law. *Majallah-yi Talim o Tahqiq, 4*, 170–183.

Anti-Rape (Investigation and Trial) Act, 2021 (Pakistan).

Electronic Transactions Ordinance, 2002 (Pakistan).

Investigation for Fair Trial Act, 2013 (Pakistan).

National Forensics Agency Act, 2024 (Pakistan).

Pakistan Single Window Act, 2021 (Pakistan).

Payment Systems and Electronic Fund Transfers Act, 2007 (Pakistan).

Prevention of Electronic Crimes Act, 2016 (Pakistan).

Protection of Pakistan Act, 2014 (Pakistan).

Qanun-e-Shahadat Order, 1984 (Pakistan).

Stamp Act, 1899 (Pakistan).

Virtual Assets Ordinance, 2025 (Pakistan).

Fakhar Zaman v. State, 2021 SCMR 1815 (Pakistan).

Hamna Qaiser v. Chairman PEMRA, 2024 MLD 243 (Pakistan).

Meera Shafi v. Federation of Pakistan, PLD 2022 Lahore 773 (Pakistan).

Rana Muhammad Arshad v. Federation of Pakistan, PLD 2021 Islamabad 42 (Pakistan).

Government of Pakistan. (2018). *Digital Pakistan policy*.

Government of Pakistan. (2018). *National artificial intelligence policy*.

Business Recorder. (2017, August 4). Conference on law and technology. https://fp.brecorder.com/2017/08/20170804205160/

Dawn. (2018, February 23). Misuse of Qanun-e-Shahadat discussed. https://www.dawn.com/news/1348889

ProPakistani. (2011, January 10). A country without cyber law: Pakistan. https://propakistani.pk/2011/01/10/a-country-without-cyber-law-pakistan/