JOURNAL OF LEGAL STUDIES
"Vasile Goldiș" Western University of Arad
J. L. S.
2026 – 38(52)
DOI: 10.2478/jles-2026-0011

DIGITAL EVIDENCE AND TRANSNATIONAL CHILD SEXUAL ABUSE: RECONSTRUCTING PAKISTAN'S JURISDICTIONAL AND INVESTIGATIVE FRAMEWORK THROUGH LESSONS FROM SINGAPORE

Muhammad Imran Ali*
Principal Quaid-e-Azam Law College, Kasur, Pakistan
E-mail: principal.kasur@qlc.edu.pk
ORCID: https://orcid.org/0000-0003-1395-229X

(Received: September 2026; Accepted: October 2026; Published: November 2026)

Abstract: Digital technologies have now made child sexual abuse a cross-border issue, making it more complex for criminal jurisdiction, evidence preservation and cross-border investigations. The article explores the legal and institutional framework in place in Pakistan for the preservation, authentication and adduction of digital evidence in transnational child sexual abuse cases and offers comparative lessons from Singapore. It critically compares Pakistan's legal regimes for jurisdiction, evidence, investigation, and international cooperation with Singapore's integrated regime through doctrinal and comparative legal analysis. The article highlights the ongoing problems in Pakistan in relation to extraterritorial jurisdiction, volatile evidence preservation, digital forensics, chain of custody, foreign-held electronic evidence, institutional coordination and platform cooperation. It maintains that these gaps enable technologically advanced criminals to take advantage of jurisdictional complexity and the time it takes to obtain evidence. Based on Singaporean practice, the article suggests a Substantial Digital Connection Test for jurisdiction, cross-border preservation and disclosure processes, harmonized digital-evidence processes, dedicated investigative capacity and increased public–private collaboration, and powers for judicial oversight of investigations. It creates a rights-based reform model balancing child protection, privacy, due process and evidentiary integrity, shifting the approach of Pakistan's response from a reactive cybercrime enforcement one to a positive transnational digital justice one.

Keywords: Child Sexual Abuse; Digital Evidence; Digital Forensics; Pakistan; Singapore.

* Corresponding author: Muhammad Imran Ali. *E-mail: principal.kasur@qlc.edu.pk*

Copyright © 2026 The Author(s). Published by VGWU Press
This is an Open Access article distributed under the terms of the Creative Commons BY 4.0 license (Creative Commons — Attribution 4.0 International — CC BY 4.0) which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Journal of Legal Studies Volume 38 Issue 52/2026
ISSN 2457-9017; Online ISSN 2392-7054.
Web: publicatii.uvvg.ro/index.php/jls. Pages 1 – 20

1. Introduction

The criminal jurisdiction has been undermined by the digitalization of child sexual abuse (CSA), as the perpetrators, victims, platforms, devices, financial transactions, and evidence of CSA can be transferred to multiple States (Lannier, 2026). This fragmentation poses a challenge: territorial sovereignty is limited, and evidence and wrongful behaviour are transnational (Ali, 2026).

The digital evidence, such as images, video, encrypted communications, IP logs, device artifacts, cloud records, payment trails, and platform metadata, can be used to prove identity, conduct, knowledge, and intent (Chand, Sharma & Kabir, 2025). It is a source of evidence that has to be found, preserved, authenticated, maintained in an unaltered state and kept in continuity. Under the Prevention of Electronic Crimes Act, 2016 (PECA), certain acts related to child pornography are criminalized under section 22, and section 19 is about the offence of unauthorised interception, which should not be deemed an investigative power. The meaning of the territorial application of the Act should be separated from the effects-based extraterritorial jurisdiction, which is most discussed in section 1(4) of the Act. Sections 31 and 32 also have different functions: section 31 does not cover traffic data retention by service providers but expedited preservation and acquisition. Article 164 of the Qanun-e-Shahadat Order, 1984 states that evidence that is produced by any device or technique which is in modern use or is in the process of being developed may be relied upon under the applicable rules of evidence and be subject to judicial scrutiny and the rules outlined in the case of Ishtiaq Ahmed Mirza v Federation of Pakistan (PLD 2019 SC 675). In addition, cross-border evidence may also be covered by section 42 PECA, the Mutual Legal Assistance (Criminal Matters) Act, 2020, and cooperation mechanisms (Shahzad, Imdad & Sultana, 2026).

Singapore provides a useful comparative model because its legal architecture distributes jurisdictional, investigative and evidentiary functions across distinct statutory frameworks. Child-abuse-material offences are included in the Penal Code, 1871, which includes 377BL and 377BO; the Evidence Act, 1893, has rules pertaining to electronic records, including section 116A (Chen, 2012); the Criminal Procedure Code, 2010, provides for investigative powers such as computer-access mechanisms.

From a methodological standpoint, the approach is based on a doctrinal and comparative legal approach, through five functional variables: criminalization, jurisdiction, investigation, digital evidence, procedural safeguards and cross-border cooperation. Singapore is chosen to be compared because its Penal Code, Criminal Procedure Code and Evidence Act have separate statutes legislating their respective

Journal of Legal Studies Volume 38 Issue 52/2026
ISSN 2457-9017; Online ISSN 2392-7054.
Web: publicatii.uvvg.ro/index.php/jls. Pages 1 – 20

duties (substantive, investigative and evidentiary), thus enabling a functional comparison with the legal system in Pakistan. The article is based on the primary legislation and secondary literature. The legal materials examined in this study are limited to those available as of 30 September 2026. The comparison does not make any assumption of institutional equivalence between Pakistan and Singapore but rather asks if selected Singaporean mechanisms can be adapted to be consistent with the institutional framework in Pakistan as well as its constitutional and statutory procedures.

2. Conceptualizing Transnational Child Sexual Abuse in the Digital Environment

The digital environment is witness to a new type of transnational child sexual abuse that transcends the concept of territorial crime and extends to a crime that is distributed across platforms, devices and jurisdictions. Online initiation, technology-enabled abuse, cross-platform offending, and digital perpetuation can include victims, offenders, service providers, payment channels, and stored data from various States (Ali, 2024). Child Sexual Abuse Material (CSAM) is thus more broadly defined than the term "child pornography" to include images, videos, livestreams, recordings, manipulated and digitally created sexually exploitative content (Quayle, 2021).

The substantive offences are available in Pakistan's Prevention of Electronic Crimes Act 2016 (PECA), as amended. Issues relating to child pornography are covered in section 22; child cyberbullying, grooming and related conduct are addressed in section 22A; offences against modesty are covered in section 21; and unlawful online content is covered in section 37.

The term child sexual abuse material (CSAM) is used to describe sexually exploitative material involving a child, whether it is created, recorded, transmitted or stored in digital format. Sections 377A and 377B of the Pakistan Penal Code are still applicable to offences of sexual abuse (Shah, 2024). However, there needs to be a differentiation between jurisdiction and substantive criminalization. Section 1(3) PECA relates to the territorial application of the Act, and section 1(4) mainly provides the basis for extending the application of the Act to the conduct of specified nature happening outside Pakistan. Section 19 of PECA makes it an offence to intercept without authorization, but does not provide for the existence of an investigative interception power. Article 164 of the Qanun-e-Shahadat Order, 1984 lays down an enabling provision for evidence produced with the help of modern devices or techniques, while maintaining the same principles upheld for traditional

evidence and subjecting them to the same requirements of judicial scrutiny with respect to authenticity, tampering and proof (Saeed & Gillani, 2021).

Beyond the production or dissemination of child sexual abuse material (CSAM), technology-facilitated abuse refers to a variety of other types of abuse, including grooming, livestreaming, sexual extortion, surveillance, impersonation, and image-based exploitation (Kaya & Erdem, 2026). These activities can leave evidence and effects at several sovereign sites, leading to overlapping legal and investigative interests. Singapore does have its own set of laws governing the substantive offence (its Penal Code), investigative powers (its Criminal Procedure Code 2010), and rules of evidence (its Evidence Act 1893) (Mohan & Lee, 2020). This digital evidence and jurisdiction connection must be considered alongside the connecting factors relevant to the law, the lawfulness of its investigation, cross-border cooperation and the admissibility of evidence gathered across borders.

3. Digital Evidence in Transnational Child Sexual Abuse Investigations

Digital evidence plays a key role in the investigation and prosecution of transnational child sexual abuse. It can be preserved, acquired, examined, authenticated, disclosed, and evaluated in court to establish identity, chronology, communications, intent and territorial connections (Franssen & Tosza, 2025). It is often the relationship between the various digital artifacts that gives it its probative value, not just one artefact on its own.

The relevant investigative mechanisms are available in the Prevention of Electronic Crimes Act 2016 (PECA) as amended in Pakistan. Section 30D is about the preservation of information prior to blocking or removal of online content. Section 31 is a provision for expedient preservation and acquisition in cases where information is at risk of alteration, destruction, loss, or unavailability. A written preservation requirement can be in effect for ninety days at the most, and the authorized officer must notify the Court of the acquisition within twenty-four hours (Haider, Ali & Zubair, 2023). Section 32 pertains to the retention of certain traffic data by service providers and should not be confused with Section 31 (Baloch & Abid, 2026).

Evidentiary loss could be a risk, as well as the difficulty of accessing the content legally if it is encrypted, anonymized, sent via VPN, temporary or held on a foreign cloud storage. Therefore, analytic separation of preservation, acquisition, and forensic examination should be maintained. Imaging, cryptographic hashing, timestamps, and documented handling can assist with forensic integrity and continuity, provided the relevant evidentiary requirements exist (Horsman, 2021).

Journal of Legal Studies Volume 38 Issue 52/2026
ISSN 2457-9017; Online ISSN 2392-7054.
Web: publicatii.uvvg.ro/index.php/jls. Pages 1 – 20

Under Article 164 of Qanun-e-Shahadat Order (QSO), 1984, evidence submitted through modern devices or techniques can be submitted to the court, in appropriate circumstances. It does not set out a comprehensive chain of custody and authentication regime, but leaves these questions to the applicable evidentiary principles (Zahoor, Sardar, Arif & Bannian, 2022). It is best interpreted, therefore, as an enabling rather than a strict authentication or chain of custody provision, rather than a comprehensive statutory code of authentication or chain of custody under Article 164 of the Qanun-e-Shahadat Order, 1984. The Supreme Court in the case of Ishtiaq Ahmed Mirza v. Federation of Pakistan (PLD 2019 SC 675) has highlighted the need for authenticity, free from tampering and in compliance with relevant evidentiary procedures when using modern devices. The comparative analysis thus distinguishes, however, any admissibility question from any question of investigative legality.

Singapore's Criminal Procedure Code 2010 and the Evidence Act 1893 separate investigative and evidentiary powers, such as powers to access computers and to decrypt data, under sections 39 and 40, respectively, as well as provisions on electronic evidence (Chen & Chua, 2018). This serves as a basis for comparison in creating Pakistan's preservation policy, legal cross-border acquisition, forensic integrity and evidence policy.

4. Pakistan's Jurisdictional and Investigative Framework

The government's approach to transnational child sexual abuse is both territorial criminal jurisdiction and a set of rules concerning digitally mediated activity that transcends borders. Section 1(3) PECA is not an umbrella clause for actions taken outside Pakistan. The principal rule based on the effects is enshrined in section 1(4), which applies when the conditions of section 1(4) are satisfied, including the effect on a person, property, information system or data in Pakistan. This may necessitate foreign evidence and international collaboration, especially to prove that certain aspects of the alleged conduct are located outside Pakistan (Saleem, Bukhtiar, Zaheer & Farooq, 2025).

Child sexual abuse material (CSAM) is defined in Section 22 PECA as the creation, distribution, transmission, procurement and possession of "sexually explicit videos, images or text" of a child under the age of 18 that has been filmed, recorded or published to or in connection with internet communication. In Section 30D, there is a focus on information preservation before blocking or removal. Section 31 covers expedient preservation and acquisition when data may be subject to alteration, loss, destruction or inaccessibility; and Section 32 covers traffic-data retention.

The application of PECA is not an alternative to the general criminal law, but it complements the Pakistan Penal Code, 1860, and the Code of Criminal Procedure, 1898. Therefore, depending on the alleged conduct, more than one statutory framework might be relevant to a digitally facilitated offence. The production of documents or things is specified in section 94 CrPC, while search procedures are specified in section 165 of the CrPC. These should not be used as the grounds for medical examination or DNA evidence. Sections 164A and 164B CrPC cover the medical examination and taking of certain forensic specimens. Such statutory differences are significant to make sure investigative processes are permitted by the correct legal provisions.

Coordinated collaboration among investigators, prosecutors, courts, telecommunications providers, and forensic laboratories is essential to effective investigation. But problems with institutional protocol, inconsistent forensic tools, slow preservation of digital evidence, encryption, and lack of cooperation from online platforms and foreign cloud-service providers can still delay investigations. (Ahmed, Rehman & Ali, 2025).

Evidence is also cross-border, with coverage of section 42 PECA, the Mutual Legal Assistance (Criminal Matters) Act, 2020, MLA processes, expedited preservation, platform cooperation and international police channels. Article 164 of the Qanun-e-Shahadat Order 1984 provides for the admissibility of evidence tendered through the use of a modern device or method. Authentic documents, evidence of tampering and proof must be subject to certain principles of evidence and be the subject of judicial examination.

5. Singapore's Regulatory and Investigative Architecture

The regulatory approach to CSE in Singapore caters to the problem from different but complementary angles: child sexual abuse substantive criminalization, child sexual abuse jurisdiction, investigation and evidence (Young, Mustafa, Rozubi, et al., 2026). Section 377C of the Penal Code 1871 outlines the definition of "child abuse material", and sections 377BG to 377BK outline conduct relating to the production, distribution, sale, offering, acquisition, viewing and possessing of such material. This concept captures the digital exploitation chain, but does not conflate the categories of offences.

There is a distinction between criminalization and the rules of jurisdiction about the prosecution of an offence. The Penal Code Section 377BL on "abusive material" and a "minor" aged 16 or older but under 18 should not be defined as an all-encompassing extraterritorial jurisdiction provision. Section 377BO is an anti-child-abuse-material offence section tailored to cases that occur overseas or overseas for part, and contains

Journal of Legal Studies Volume 38 Issue 52/2026
ISSN 2457-9017; Online ISSN 2392-7054.
Web: publicatii.uvvg.ro/index.php/jls. Pages 1 – 20

a number of statutory circumstances under which Singapore's criminal jurisdiction can apply. It is not only possible to assess its operation by reference to the relevant subsections and their connecting factors, but this must be done, and a broad interpretation of a 'digital relationship' is not sufficient. An additional basis of jurisdiction may be provided by section 13 of the Computer Misuse Act where its conditions are met. Hence, territoriality and the specific statutory connections are still relevant for establishing jurisdiction over transnational behaviour (Chan, Lysaght, Lim, Toh & Savulescu, 2024).

Investigators have specific powers as stipulated in the Criminal Procedure Code 2010. Section 20 allows the making of written or electronic records. Access to computers (including computers outside Singapore) is granted under section 39 in prescribed circumstances, and access to information for decryption is granted under section 40. These are investigative powers different from the rules of evidence.

The Evidence Act 1893 regulates matters of evidence, such as section 116A, which provides for a rebuttable presumption in respect of records created or communicated using electronic systems, which must be evaluated by the judge.

The Singapore Police Force, the Attorney-General's Chambers, relevant authorities and technology platforms cooperate with each other in the investigation, preservation requests, mutual legal assistance and international police cooperation (Khan, 2024).

The current Pakistani system should be separated from the proposed changes. The *lex lata* refers to the jurisdictional, investigative, evidentiary and cooperation provisions currently in place under the Prevention of Electronic Crimes Act (PECA), 2016, the Qanun-e-Shahadat Order (QSO), Pakistan Penal Code (PPC), the Code of Criminal Procedure (CrPC) and the Mutual Legal Assistance (Criminal Matters) Act, 2020. Lack of effectiveness in implementing those mechanisms does not give new powers. The proposed reforms in this article are therefore *de lege ferenda*. That is, they are a suggestion for how things could be done better, not a law as currently in force.

6. A Comparative Analysis: Pakistan and Singapore

Pakistan and Singapore have different, but complementary, strategies for addressing transnational digital child sexual abuse. In Pakistan, sections 22 and 22A-22C PECA, along with relevant provisions of the Pakistan Penal Code (PPC), criminalize certain child-related online behaviours and sexual activities. Section 1(3) relates to the territorial scope of the Act, and section 1(4) relates mainly to the effect-based application of PECA to a specified act abroad where the conditions set out in the Act

are present. While section 31 focuses on the accelerated preservation and acquisition of data, section 32 relates to service providers' retention of specific traffic data, but does not provide general investigative access and copying powers. According to Article 164 of the Qanun-e-Shahadat Order, 1984, modern devices and techniques can be used for obtaining evidence if they are a reliable and credible means and have been authenticated before use in court. Cross-border investigations are also available under Section 42 PECA and pertinent mutual legal assistance mechanisms.

Extraterritorial application of certain child-abuse-material offences is provided for in Singapore law. The child-abuse-material offences are contained in sections 377BG-377BK of the Penal Code, and the specified exploitation involving abusive material and a minor (16 years or older but under 18 years) is contained in Penal Code section 377BL. Under Section 377BO, 'Child abuse material offences outside or partially outside Singapore', Singapore criminal law can be invoked in relation to offences committed outside or partly outside Singapore under various circumstances. The following circumstances are statutory connections: connection to the accused; geographical connection (where was the conduct); connection to the child (where was the child; how old was the child). The provision should not be paraphrased as only resulting in 3 different configurations; the scope of the provision must be interpreted and analyzed through the relevant subsections and offence provisions. The jurisdictional inquiry will thus proceed not based on the content of online information or digital content being generally available in Singapore, but based on the statutory criteria.

The comparison shows that PECA can lay the foundations for combating transnational digital child sexual abuse but can be improved with more specific statutory 'connecting factors' and better integration with digital evidence preservation and the collection of foreign evidence and international cooperation. Singapore's s.377BO provides an example of legislation that expressly provides for cases where actions committed outside Singapore are also covered by the local criminal jurisdiction.

Table 1. Comparative Jurisdictional Connecting Factors in Pakistan and Singapore

Functional variable	Pakistan	Singapore
Criminalisation	PECA ss.22, 22A–22C and relevant PPC provisions criminalize specified child-related cyber and sexual conduct.	Penal Code ss.377BG–377BK address specified child-abuse-material offences; s.377BL addresses exploitation by abusive

		material involving minors aged 16–17.
Jurisdiction / connecting factors	PECA s.1(3) concerns territorial application; s.1(4) principally provides an effects-based basis for specified extraterritorial conduct.	Penal Code s.377BO provides multiple statutory circumstances for extraterritorial or partly extraterritorial application.
Nature of territorial connection	The statutory connection may include specified effects on a person, property, information system, or data in Pakistan.	Statutory connections depend on the applicable subsection, including the accused, location of conduct, and child's location and age.
Preservation/investigation	PECA s.31 addresses expedited preservation and acquisition; s.32 concerns traffic-data retention by service providers.	Investigative powers are governed by the applicable criminal procedure and other statutory provisions.
Digital evidence	Article 164 of the Qanun-e-Shahadat Order 1984 permits evidence obtained through modern devices and techniques, subject to judicial evaluation of authenticity and reliability.	Electronic and digital evidence may be considered under applicable evidentiary and procedural rules.
Cross-border cooperation	PECA s.42 operates alongside applicable MLA and law-enforcement cooperation mechanisms.	Singapore uses MLA and international law-enforcement cooperation mechanisms to obtain foreign evidence and support transnational investigations.
Comparative significance	The framework provides a basis for transnational enforcement but would benefit from more expressly defined jurisdictional connections and integrated cross-border procedures.	Section 377BO provides a detailed statutory model in which extraterritorial jurisdiction is tied to identifiable connections involving the offender, the child and the location of conduct.

The comparison shows a difference in how jurisdiction is defined in the statutes. The main basis provided in Pakistan for applying the Act to some conduct abroad is the specified effects under PECA section 1(4). The Singapore Penal Code section 377BO, on the other hand, lays out several circumstances where the specified child-abuse-material offences may be applied to actions that take place abroad or partly abroad. The jurisdictional relations should be determined from the relevant statutory provisions – of the accused, where the conduct occurred, where the child was, and his or her age at the time of the conduct. The comparative implication for Pakistan is whether it is possible to establish clear, statutory connecting factors, along with the preservation of digital evidence, foreign-evidence processes, international cooperation, and safeguarding of procedures, to increase predictability and jurisdiction. Digital accessibility should not be considered a satisfactory basis for jurisdiction.

The comparative lesson for Pakistan should be that it does not need to copy the Singapore framework exactly but to reflect on whether there are more specific connecting factors – statutory in nature – which could clarify under which circumstances transnational digital child sexual abuse is subject to the jurisdiction of Pakistan.

7. Reconstructing Pakistan's Jurisdictional Framework for Transnational Digital Abuse

The territorial approach should not be neglected, and the jurisdictional framework for transnational digital child sexual abuse should be evaluated using explicit statutory links. Offenders, victims, platforms, infrastructure and evidence of digitally-mediated abuse can be spread across national borders. Section 1(3) PECA is about the territorial application of the Act, while section 1(4) PECA primarily sets the basis for the application of the Act to specified conduct outside Pakistan where the statutory conditions are met, in the context of its effects. Sections 22 and 22A-22C of the PECA criminalize specific acts involving children and pornography. Section 19 is about the offence of unauthorized interception and does not have the same powers of investigation as are elsewhere in the statutory framework. Any proposed Substantial Digital Connection Test should therefore define the jurisdictional connection in a manner that does not misinterpret the current statutory powers, or exceed them.

The proposed framework should clearly include significant links such as the location of victims, harm, the use of Pakistani devices, accounts, financial channels, data, or deliberate targeting of activities towards Pakistan. Criminal jurisdiction should not

Journal of Legal Studies Volume 38 Issue 52/2026
ISSN 2457-9017; Online ISSN 2392-7054.
Web: publicatii.uvvg.ro/index.php/jls. Pages 1 – 20

be based on platform availability, but on the need to assess those who played a significant part, facilitated, were aware of or chose not to satisfy their legal obligations to preserve or disclose the platform.

Concurrent jurisdiction can exist when a state and another state have a relationship to aspects of the alleged conduct, and/or aspects of the conduct occurred in more than one state, and/or when the accused and/or the victim are connected to more than one state, or aspects of the crime took place on a digital infrastructure that has a relationship to more than one state. The presence of these connections is not sufficient to impute guilt for the offence to the accused. To establish attribution, there must be supporting digital and traditional evidence, including subscriber details, IP logs, device artifacts, platform records, financial evidence and witness statements (Jain, Aggrawal, Dangi, Shukla, Yadav & Choudhary, 2025). The jurisdictional basis, and the evidence available for prosecution, should thus be examined on a separate basis.

The proposed Substantial Digital Connection Test is not designed to provide a standalone basis for criminal jurisdiction, but rather to make section 1(4) PECA's existing effects-based jurisdiction more certain. It is intended to locate material and reasonably foreseeable avenues for aid in prosecuting and courts assessing cross-border activity. Any use of the test has to be consistent with statutory authority, legality, foreseeability, proportionality, comity and procedural fairness. The test is suggested as an analytical tool for determining jurisdiction and not as a replacement for the jurisdictional statutes of the offence and/or the jurisdiction of the particular court.

Singapore makes a comparative reference to Penal Code 1871, section 377BO on specified extraterritorial conduct of child abuse material. The Substantial Digital Connection Test, which it is proposed should be required, should be met by the following: (1) a Pakistani victim or harm; (2) a Pakistani connection, either intentional or reasonably foreseeable; and (3) the use of 'substantial Pakistani digital infrastructure.'

Statutory provisions and the principle of international cooperation should govern the application of the concurrent criminal jurisdiction. Articles 4 and 10A of the Constitution of Pakistan offer key local benchmarks for the treatment of individuals in accordance with the law and the right to a fair trial (Majeed, Khan & Asif, 2022). The requirements of a fair trial in international and Pakistani legal framework: A critical analysis. Pakistan Languages and Humanities Review, 6(1), pp. 193–203. The principles of legality and foreseeability must be satisfied when it comes to

criminal liability and the basis for prosecution; this means that criminal liability and the jurisdiction for prosecution must be clearly and reasonably foreseeable (Aleissa, Al Wahshat, Balas, Asouli, & Alshamayleh, 2023). The doctrine of *ne bis in idem* must be applied in accordance with the domestic law of the state in which the proceedings or judgments are pending and must not be interpreted as to serve as a general bar to concurrent proceedings in the various states; if proceedings or judgments have been instituted in another jurisdiction, that fact shall be taken into consideration (Gellér, 2025). Coordinating between the states which assert jurisdiction may be achieved through comity, but it is not the comity itself that constitutes the determination of the jurisdictional question. These should guide a sensible evaluation of the relationship with Pakistan, fairness of proceedings and cooperation with foreign authorities.

8. Reconstructing Pakistan's Digital Investigative Framework

An investigative architecture is needed in Pakistan to transform volatile digital traces into admissible evidence. PECA 2016 lays a procedural background. Namely, Section 30D is about the investigation of child sexual content referred to the Pakistan Telecommunication Authority; Section 31 is about expedited preservation and acquisition where the data is likely to be modified, lost, destroyed, or inaccessible, and acquisition shall be brought before the Court within 24 hours of giving notice; Sections 33 and 34 focus on warrants for search and seizure and disclosure of data content; Section 40 is about the forensic laboratories; Section 42 is about international cooperation. Section 32 regulates the retention of traffic data, and should not be confused with preservation.

The security of data should be achieved through preservation; acquisition should be limited to lawful authority and necessity, proportionality, integrity and judicial oversight. Imaging, hashing, extraction, documentation, storage, transfer and examination should be standardized and be part of forensic protocols. The chain of custody should contain the names of the people involved in the collection, date and time of collection, methods used, hash values, storage conditions, and subsequent handlers and analytical changes. Article 164 of the Qanun-e-Shahadat Order, 1984, is an enabling provision for the use of modern devices/tics for the production of evidence, and the authenticity, integrity and reliability of the evidence are to be determined by law and judicial standards.

To achieve this, a coordinated approach involving section 42 of PECA, the Mutual Legal Assistance (Criminal Matters) Act, 2020, urgent preservation requests, platform co-operation and international police channels must be used to obtain cross-

Journal of Legal Studies Volume 38 Issue 52/2026
ISSN 2457-9017; Online ISSN 2392-7054.
Web: publicatii.uvvg.ro/index.php/jls. Pages 1 – 20

border evidence. Singapore is used as a reference in the Criminal Procedure Code 2010 (production and computer access).

Cybercrime-child protection cells comprising investigators, prosecutors, forensic analysts, child-protection professionals and international-cooperation officers should be set up in Pakistan. Reporting and lawful-disclosure obligations should be outlined on the platform. AI-assisted hashing and pattern recognition may create investigative leads that lead to the identification of CSAM, but results should be treated as investigative leads and verified, documented, reviewed by judges and minimized. The proposal should therefore be understood as an institutional reform of timing and coordination, not as an assertion that Pakistan's present law already contains a separate preservation order of this kind.

9. Cross-Border Evidence, Mutual Legal Assistance, and International Cooperation

With cloud computing, one can expect data to come from a country other than Pakistan, pass through another country's infrastructure, reside distributed among different jurisdictions, and be managed by providers in other countries. Therefore, cross-border child sexual abuse investigations will require integrated, coordinated authorities to ensure that evidence is preserved, collected and authenticated, especially as evidence of a volatile nature can be lost before the formal processes are completed.

Under Section 42 PECA 2016, international cooperation in relation to electronic evidence is given a statutory footing, and under the Mutual Legal Assistance (Criminal Matters) Act, 2020 (Act No. XXII of 2020), the general domestic framework for international cooperation in relation to the formal provision of mutual legal assistance is established. The latter creates a central body and methods for providing evidence and other support from abroad. It is important, therefore, that section 42 PECA works in parallel with the MLA framework and not replace it.

So, a two-tier approach is suitable: expedite preservation, then disclose. Preservation requests must go through specially established channels of communication (24/7) to ensure that subscriber records, IP logs, metadata or content held on the platform do not get deleted. Further disclosure shall be consistent with the requirements of judicial authorization, proportionality, limitation on purpose, authenticity and protection of privacy. This distinction will prevent the informal evidence acquisition, which is termed emergency preservation, from being confused with the formal evidence acquisition (Keenan, 2025).

A relevant institutional comparison is Singapore's Mutual Assistance in Criminal Matters Act 2000 (MACMA), which provides a statutory form of mutual assistance in criminal matters. The Act has provisions for support in the acquisition of evidence and other types of investigative cooperation, based on the provisions and requirements under the law. It should be referred to in terms of the form of assistance being considered, whether taking of evidence, production, search and seizure or authentication. Formal requests must be made through the competent authority in line with the provisions of the Act and procedures.

Co-ordination between the central authority, investigators, prosecutors, courts, foreign police, platforms and international police should, therefore, be enhanced in Pakistan. Automated preservation notice, electronic transmission of the notice, and emergency child-protection measures may be useful in speeding up the cooperation process, but without compromising judicial protection. There are other normative and operational reference points like the Budapest Convention and INTERPOL mechanisms. The goal is a transnational evidence regime of speedy preservation, formalized MLA processes, platform collaborations, authentication, privacy and judicial controls.

Under Section 42 PECA, international cooperation is afforded a statutory basis on electronic evidence, while the Mutual Legal Assistance (Criminal Matters) Act, 2020 provides a domestic framework for formal mutual legal assistance. Expeditious preservation can be employed to avoid loss of volatile information during the process of initiating a formal preservation process and should not be considered a replacement for the rules of disclosure and evidentiary transfer. It is important to recognize that formal mutual legal assistance is different from platform cooperation and international police channels, which can support but are not the same as formal mutual legal assistance.

10. Reconciling Child Protection, Privacy, and Due Process

Child protection, privacy and due process should be interrelated parts of the digital criminal justice process. The constitutional protections of life and liberty, fair trial and due process, dignity and privacy and special protection of children are outlined in Articles 9, 10A, 14 and 25(3) of the Constitution of Pakistan. Cyber-investigative measures relating to children must therefore have legitimate protective purposes and be necessary and proportionate, and subject to legal and judicial safeguards.

PECA 2016 has a number of child protection and investigative safeguards. Sections 30B and 30C mainly cover the protection of victims and witnesses and in-camera trials, and section 30D covers the investigation and acquisition of content relating to child sexual abuse referred for blocking and removal. Section 31 separately refers to

the acquisition and preservation of specified data through expedition, and section 32 refers to the retention of specified traffic data by service providers. Provision must also be made for search, seizure and disclosure powers to be used in accordance with the provisions of the various aspects of warrants and judicial supervision. These provisions must not be interpreted as unlimited investigative powers, but are subject to the principles of necessity, proportionality, respect for the child's privacy and best interests.

The process of evidence gathering should also avoid a second exposure to victimization. Investigators should avoid unnecessary disclosure of identifying information or uncontrolled duplication or circulation of CSAM, and avoid repeated interviews. Therefore, there is a need for secure forensic environments, limited access, documented handling procedures and appropriate integrity control. Article 164 of the Qanun-e-Shahadat Order, 1984 affords an enabling basis for courts to accept evidence presented by means of modern methods or devices; however, it does not provide a complete legislative framework of authenticity or chain of custody. The principles of Pakistani jurisprudence, especially in the case of Ishtiaq Ahmed Mirza vs Federation of Pakistan (PLD 2019 SC 675), are that audio or video evidence should be produced as evidence of the truth of the matter, be free from tampering and comply with the law of evidence in all other respects.

Singapore offers an example of how child protection and procedural safeguards can coexist. It has an aspect of criminal procedure that offers procedures for the use of child evidence, and has an aspect of data protection that governs the collection, use, disclosure, security, retention and transfer of information to other countries of personal data. Sections 13, 17, 18, 24-26 of the Personal Data Protection Act 2012 (PDPA) provide examples of the principles of lawful processing, purpose limitation, security, retention and cross-border protection.

AI-generated leads should not be taken as their own justification for intrusive action but should still be treated as investigative leads to be verified by humans and lawfully backed with evidentiary proof. Moreover, in the context of rights analysis, the distinction is to be drawn between powers as they are currently in force (*lex lata*) and proposed safeguards and mechanisms, *de lege ferenda*. There is the legal context under existing constitutional and statutory protection, in which the powers of investigation operate. These safeguards are especially vital when the evidence of CSAM includes a significant amount of highly personal information about children and when investigative duplication may also inflict further harm upon children's privacy and dignity.

This framework should balance effective investigation with privacy, dignity, and fair trial and evidentiary reliability. These are among the existing safeguards recognized by the lex lata analysis of the article and should be given in isolation as proposals of *de lege ferenda* for reinforcing their effective coordination in transnational digital child-exploitation cases.

11. Towards a Singapore-Informed Reform Model for Pakistan

Pakistan is in need of a coherent reform architecture between jurisdiction, investigation, evidence, institutional capacity and international cooperation. There are existing sources of information regarding child sexual abuse that are relevant to PECA 2016: Section 22 criminalizes the specified child sexual abuse material, Sections 30B-30D provide victim, witness and procedural protections, Section 31 is about expedient preservation and acquisition, Section 32 is about retention of specified traffic data, Sections 33-35 are about investigative measures, Section 40 is about forensic laboratories, Section 41 is about protecting confidentiality, and Section 42 is about international cooperation. These should be analytically separated into substantive, procedural and evidentiary aspects.

The current statutory framework that supports the extraterritorial application of PECA is mainly enshrined in section 1(4), which deals with specified conduct outside Pakistan which meets statutory effects-based conditions. Section 1(3) is not meant to be the general provision covering offences committed overseas. The proposed Substantial Digital Connection Test aims to provide a framework for evaluating the relevant connections such as the victim's location, the foreseeable impact in Pakistan, deliberate targeting and significant use of Pakistani digital infrastructure. It must be used in a manner consistent with lawfulness, predictability, proportionality, comity and procedural fairness. The issue of ne bis in idem must be based upon the applicable domestic law and international arrangements rather than taken for granted between jurisdictions.

At the institutional level, Pakistan should have a dedicated Cyber Crime Unit for children, comprising investigators, prosecutors, forensic computer scientists, and Child Protection Specialists with a dedicated 24/7 Child Preservation and International Evidence Collection Unit. The proposed rapid preservation mechanism should not abrogate or replace section 31 and should be subject to judicial notice and proportionality and temporal limitations.

Secure forensic handling, metadata preservation, integrity verification and authentication and documented custody should be enhanced in evidentiary reform. The words of Article 164 of Qanun-e-Shahadat Order, 1984 ought to be considered an enabling provision for modern evidence, which should be supplemented by

legislation where required and/or guided by the case of Ishtiaq Ahmed Mirza v Federation of Pakistan (PLD 2019 SC 675) in Pakistani jurisprudence.

The cross-border reform should be integrated with the Mutual Legal Assistance (Criminal Matters) Act, 2020, the platform cooperation and international police channels, and inform the preservation procedure as per section 42 PECA. Singapore provides an institutional comparison, but is not a model for wholesale transplant.

First, the lex lata defines the existing architecture of the law, in that it outlines the provisions of PECA sections 1(3), 1(4), 22, 30B–30D, 31, 32, 33–35, and 40–42, as well as Article 164 of the Qanun-e-Shahadat Order, 1984, and the Mutual Legal Assistance (Criminal Matters) Act, 2020, and related provisions of the criminal law and procedure. Second, the de lege ferenda proposals aim to enhance that architecture by introducing a significant digital connection test, speeding up the coordination of the preservation, bolstering the capacity in the domain of child cybercrime, establishing a clear and stable governance of digital forensic investigation, and making platform cooperation accountable and improving the international evidence process. These categories help to make it easier to distinguish between those that represent existing law and those that are part of the article's proposed changes.

12. Conclusions

Traditional territorial approaches are not sufficient to address transnational child sexual abuse issues of jurisdiction and investigation. The framework of Pakistan should, therefore, be examined in the light of the relevant statutory connecting factors, including the effect-based extraterritorial rule in section 1(4) PECA. Other provisions of the Act apply to relevant investigative measures, and the Act differentiates between expedited preservation and acquisition under section 31 and traffic-data retention under section 32. The legal basis for international cooperation is contained in Section 42, but must be carried out in conjunction with the existing mutual legal assistance procedures. Implementing the same also involves institutional co-ordination, legal evidence management, and procedural protection.

Ensuring the reliability of digital evidence is based on an ongoing legal process: proper and timely preservation, proper and timely acquisition, proper and secure forensic examination, assessment of integrity and authenticity, proper documentation of custody, cross-border retrieval, and judicial scrutiny and admissibility. Under Article 164 of the Qanun-e-Shahadat Order, 1984, there is evidence provided by modern devices, and it should be applied consistently with

Pakistani jurisprudence on evidence, including the case of Ishtiaq Ahmed Mirza vs Federation of Pakistan (PLD 2019 SC 675).

There's no need for Pakistan to emulate the Singaporean legal framework entirely. Singapore's model of jurisdiction, investigation, evidence and international cooperation, however, provides valuable guidance. Pakistan should ensure that the procedures are child-centred, that the evidence is preserved in a lawful manner in a timely manner, that investigations are special, that the platforms cooperate in an accountable manner and that international assistance is provided effectively, while respecting the privacy, dignity and fair-trial rights of children.

The value of the article in the scientific context is the link it makes between jurisdictional analysis and the evidentiary life cycle of transnational child sexual abuse, rather than considering jurisdiction, investigation and digital evidence as separate issues.

Acknowledgements

The author thanks the anonymous reviewers and editor for their valuable contribution.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not – for – profit sectors.

Author Contributions

The entire article has been written by Muhammad Imran Ali.

Disclosure Statement

The author has no competing financial, professional, or personal interests from other parties.

References

1. Ahmed, I., Rehman, T. U., & Ali, S. H. (2025). Digital evidence in Pakistan: Legal framework, forensic challenges, and judicial reliability. *Contemporary Journal of Social Science Review, 2(1)*, pp. 12-20.
2. Aleissa, T. Y., Al Wahshat, Z. M., Balas, H. A. M., Asouli, S. A. R. S., & Alshamayleh, G. M. Y. (2023). Principle of legality in international criminal law. *Pakistan Journal of Criminology, 15(4),* pp. 683-694.
3. Ali, M. I. (2024). Strategies for intervention and prevention in online child sexual exploitation. *Teisė, 132,* pp. 145-155.

4. Ali, M. I. (2026). Unmasking anonymity: Thorn's approach to combating online child sexual exploitation in India and its adaptability to Pakistan's legal framework. *Journal of Legal Studies, 37(51),* pp. 81-97.

5. Baloch, A., & Abid, D. A. (2026). Effectiveness of cybercrime legislation and enforcement mechanisms in Pakistan: A mixed-method evaluation of PECA 2016, legislative reforms, and the National Cyber Crime Investigation Agency (NCCIA). *Social Science Review Archives,* 4(2), pp. 2142-2158.

6. Chan, H. Y., Lysaght, T., Lim, X. X., Toh, H. J., & Savulescu, J. (2024). Accessing third-party research databases for criminal investigations: Enhancing legal protections and safeguarding public interests. *Medical Law International, 24(2),* pp. 97-127.

7. Chand, R. R., Sharma, N. A., & Kabir, M. A. (2025). Advancing web browser forensics: Critical evaluation of emerging tools and techniques. *SN Computer Science, 6,* 355. https://doi.org/10.1007/s42979-025-03921-6

8. Chen, S. (2012). Reliability and relevance as the touchstones for admissibility of evidence in criminal proceedings: Muhammad bin Kadar v PP [2011] 3 SLR 1205 [Case Note]. Singapore *Academy of Law Journal, 24(2),* pp. 535-554. https://ink.library.smu.edu.sg/sol_research/1979

9. Chen, S., & Chua, E. (2018). 2018 changes to the Evidence Act and Criminal Procedure Code-The Criminal Justice Reform Bill and Evidence (Amendment) Bill. *Singapore Academy of Law Journal,* pp. 1-31. https://ink.library.smu.edu.sg/sol_research/2796

10. Franssen, V., & Tosza, S. (Eds.). (2025). Collecting digital evidence: Transversal challenges and solutions. In *The Cambridge Handbook of Digital Evidence in Criminal Investigations* (pp. 11-218). Cambridge: Cambridge University Press.

11. Gellér, B. J. (2025). The principle of ne bis in idem and the European arrest warrant as vehicles for the CJEU for redefining the powers of national prosecutions in EU law. *Frontiers in Sociology, 10,* 1546825. https://doi.org/10.3389/fsoc.2025.1546825

12. Haider, W., Ali, A., & Zubair, M. (2023). Prevention of Electronic Crime Act, 2016: An Analysis of the Act's Effectiveness in Controlling Misuse of Social Media in Pakistan. *Journal of Educational Research & Social Sciences Review, 3(2),* pp. 48-54.

13. Horsman, G. (2021). A case study on anonymized sharing platforms and digital traces left by their usage. *Science & Justice, 61(1),* pp. 97-106. https://doi.org/10.1016/j.scijus.2020.09.002

14. Ishtiaq Ahmad Mirza v. Federation of Pakistan, 2019 PLD 675 (S.C. Pakistan).

15. Jain, V. K., Aggrawal, J., Dangi, R., Prasad Shukla, S. S., Yadav, A. K., & Choudhary, G. (2025). Unmasking the true identity: Unveiling the secrets of virtual private networks and proxies. *Information, 16(2),* 126. https://doi.org/10.3390/info16020126

16. Kaya, K., & Erdem, Z. (2026). Understanding cyber grooming in children and adolescents: A scoping review of risk factors and prevention strategies. *Frontiers in Psychiatry, 17,* 1896109. https://doi.org/10.3389/fpsyt.2026.1896109

17. Keenan, B. (2025). From interception to integration: Encryption, bulk data, and the investigatory powers regime. *King's Law Journal, 36(3),* pp. 508-539. https://doi.org/10.1080/09615768.2025.2551419
18. Khan, A. A. (2024). Reconceptualizing policing for cybercrime: Perspectives from Singapore. *Laws, 13(4),* 44. https://doi.org/10.3390/laws13040044
19. Lannier, S. (2026). Obligations of online service providers to fight against child sexual abuse material-a systematization of EU law. *Victims & Offenders, 21(3),* pp. 506-534. https://doi.org/10.1080/15564886.2025.2557901
20. Majeed, N., Khan, A. N., & Asif, A. (2022). The requirements of a fair trial in international and Pakistani legal framework: A critical analysis. *Pakistan Languages and Humanities Review, 6(1),* pp. 193-203.
21. Mohan, S. C., & Lee, Y. (2020). Sexual grooming as an offence in Singapore. *Singapore Academy of Law Journal, 32,* pp. 96-123.
22. Quayle, E. (2021). Online child sexual exploitation and abuse. In J. M. Brown & M. A. H. Horvath (Eds.), *The Cambridge Handbook of Forensic Psychology* (pp. 279-295). Cambridge: Cambridge University Press.
23. Saeed, M. A., & Gillani, A. H. (2021). Evidential representation of using modern devices and decision-making feasibility in Pakistan. *Journal of Law & Social Studies, 3(2)*, pp. 79-86.
24. Saleem, H. A. R., Bukhtiar, A., Zaheer, B., & Farooq, M. A. U. (2025). Challenges faced by the judiciary in implementing cybersecurity laws in Pakistan. *The Critical Review of Social Sciences Studies, 3(1),* pp. 1052-1066.
25. Shah, S. K. A. (2024). A critical analysis of the efficacy of the Prevention of Electronic Crimes Act, 2016: Irritants and remedies. *Journal of Pakistan Administration, 45(2),* pp. 66-91.
26. Shahzad, M. K., Imdad, A., & Sultana, N. (2026). Rethinking the authentication of AI-generated evidence under Article 164 of the Qanun-e-Shahadat Order, 1984: Reforming Pakistan's evidentiary framework. *Journal for Social Science Archives, 4(1)*, pp. 2553-2570.
27. Young, A., Mustafa, M. C., Rozubi, et al., (2026). Child sexual exploitation and abuse: Considerations of cultural differences in policy and legislation. *Frontiers in Public Health, 13,* 1721238.
28. Zahoor, R., Sardar, S., Arif, W. K., & Bannian, B. (2022). Digital evidence and its admissibility under Pakistani law. *Journal of Development and Social Sciences, 3(4),* pp. 51-60.