

IN THE HIGH COURT OF SINDH AT KARACHI

Criminal Acquittal Appeal No.449 of 2025

Appellant : The State, through Mr. Mohsin Qadir Shahwani,
Addl: Attorney General a/w I.O SIP Amar Ali Khoso.

Complainant : Major Retd. Mumtaz Hussain Shah through Mr.Syed
Hasan, Advocate.

Respondent : Farrukh Thanvi, through Mr. Mohammad
Masood Khan, Advocate.

Date of hearing : 20.05.1016.

Date of judgment : 20.07.2026.

Date of announcement: 22.07.2026

J U D G M E N T

TASNEEM SULTANA, J.— Through this criminal acquittal appeal, the State has assailed the judgment dated 22.05.2025, passed by the learned Sessions Judge, Karachi South, in Criminal Appeal No.16 of 2024, whereby the appeal preferred by respondent Danish Farrukh Thanvi was allowed, the judgment of conviction and sentence dated 08.05.2024, passed by the learned Civil Judge and Judicial Magistrate-I, Karachi South, in Criminal Case No.5709 of 2019, arising out of FIR No.04 of 2019, registered at FIA Cyber Crime Circle, Karachi, under Sections 3, 4, 16, 20, 21 and 24 of the Prevention of Electronic Crimes Act, 2016, read with Section 419, P.P.C., was set aside and the respondent was acquitted of the charge.

2. Brief facts of the prosecution case are that Syeda Mehvish Ali, daughter of complainant Major (Retd.) Mumtaz Hussain Shah, had worked in Background Check Group, headed by the respondent, and was provided an official Samsung mobile phone during her employment. It was alleged that the respondent installed spyware in the said phone without her knowledge, gained unauthorized access to her Facebook, Gmail and LinkedIn accounts, extracted her photographs and other personal data and threatened to place the same on the internet. He was further alleged to have created fake Facebook profiles under the names “Maya Ali” and “Kazim Khan Shah”, displayed her photograph as profile picture, circulated her photographs with hateful and vulgar comments, transmitted obnoxious, defamatory, humiliating and sexually explicit material through email and WhatsApp and uploaded or shared an objectionable video through a link connected with a pornographic website. It was also alleged that he unlawfully obtained call-detail records relating to the complainant and his family. During inquiry, information obtained from Facebook disclosed that the profile “Kazim Khan Shah” had been created through IP address 196.194.131.38, while the corresponding internet connection stood registered in the name of Noreen Qaiser, wife of

the respondent, at his Clifton residence. A search of the said premises was thereafter conducted, during which mobile phones, a tablet, an iPhone, laptops, hard drives, portable drives and other digital articles were recovered and seized; hence, the aforesaid FIR was registered against the respondent.

3. After completion of the investigation, the Investigating Officer submitted the charge-sheet under Section 173, Cr.P.C. before the trial Court. The requisite documents were supplied to the respondent in terms of Section 241-A, Cr.P.C., whereafter formal charge was framed against him at Exh.02, to which he pleaded not guilty and claimed trial.

4. To prove its case, the prosecution examined nine witnesses: PW-01 Inspector Shagufta Ahmed at Exh.03; PW-02 Irfan-ul-Haq, an employee of the respondent's company, at Exh.04; PW-03 complainant Major (Retd.) Mumtaz Hussain Shah at Exh.05, who produced his complaints and communications submitted before FIA Islamabad as Exhs.5/A and 5/B; PW-04 Inspector Tariq Arab at Exh.06, who produced the thirty-page initial technical report as Exh.6/A; PW-05 Muhammad Aamir Zaib Khan, Digital Forensic Expert, FIA, at Exh.07, who produced the forensic report relating to the complainant-produced Samsung Galaxy J7 as Exh.7/A; PW-06 Nauman Ali, Forensic Expert, FIA, at Exh.08, who produced the forensic reports relating to the electronic devices recovered from the respondent's premises as Exhs.8/A and 8/B; PW-07 victim Syeda Mehvish Ali at Exh.09; PW-08 Sub-Inspector Imran Saad at Exh.10, who produced the relevant letter, seizure memo, forwarding letter for forensic examination and correspondence relating to Facebook as Exhs.10/A to 10/D, respectively; and PW-09 Ameer Ali Khoso at Exh.11.

5. Thereafter, the statement of the respondent was recorded under Section 342, Cr.P.C. at Exh.12, wherein he denied the allegations, claimed false implication and alleged foisting of the forensic material. In support of his defence, he produced a copy of FIR No.25 of 2017 as Mark-1; a four-page application under Section 22-A, Cr.P.C. moved by the victim as Mark-2; a four-page summary order passed in FIR No.25 of 2017 as Mark-3; his four-page complaint dated 07.01.2017 submitted before the FIA as Mark-4; and the FIA letter concerning registration of the complaint dated 08.11.2017, along with fifteen pages of annexures, as Mark-5. He did not examine himself on oath under Section 340(2), Cr.P.C., but examined Mehmood Ahmed Malik, a questioned-document expert, as DW-01 at Exh.13, who produced his opinions as Exhs.13/A and 13/B. The learned trial Court, vide judgment dated 08.05.2024, convicted and sentenced the respondent under the aforesaid provisions. However, the learned appellate Court, through

judgment dated 22.05.2025, allowed his appeal and acquitted him of the charge.

6. Learned Addl. Attorney General assisted by learned counsel for the complainant contended that the impugned judgment is based upon misreading and non-reading of the material evidence available on record; that the learned appellate Court failed to appreciate the cumulative effect of the Facebook record, IP particulars, subscriber information, mobile-number link and forensic material; that the respondent's connection with mobile No.0345-2130920 was established through his own complaint produced as Mark-4; that the same number appeared in the WhatsApp data extracted from the Samsung Galaxy J7 produced by the complainant; that PW-05 and PW-06 had examined different electronic devices, but the learned appellate Court failed to maintain that distinction while assessing their respective findings; that the objection under Section 33 of PECA did not affect the independently obtained service-provider record or the mobile phone separately produced by the complainant; and that the defence evidence did not dislodge the prosecution case. He, therefore, prayed that the impugned judgment be set aside and the judgment of conviction and sentence passed by the learned trial Court be restored.

7. Conversely, learned counsel for the respondent supported the impugned judgment and contended that the prosecution had failed to connect the respondent with the alleged unauthorized access, creation or operation of the false Facebook profiles, installation of spyware or transmission and uploading of the objectionable material; that the complaint was lodged after delay and arose out of previous hostility between the parties; that the search, seizure, custody and forensic examination of the electronic devices were not conducted in accordance with the requirements of law, particularly Section 33 of PECA; that the prosecution witnesses made material admissions during cross-examination; that the disputed documents relating to the production and forwarding of the mobile phone were not proved beyond doubt; that material circumstances were not put to the respondent during his examination under Section 342, Cr.P.C.; and that the view taken by the learned appellate Court was reasonable and did not warrant interference in an acquittal appeal.

8. Heard learned Addl. Attorney General, learned counsel for the respondent and perused the material available on record with their assistance.

9. A judgment of acquittal ordinarily strengthens the presumption of innocence in favour of an accused and is not to be interfered with merely because another view of the evidence may also be possible. Such restraint,

however, does not extend to an acquittal founded upon material misreading or non-reading of evidence. Interference is warranted where the acquitting Court has disregarded material evidence, separated mutually supporting circumstances or reached a conclusion not reasonably supported by the record. Reference may be made to Ghulam Sikandar and another v. Mamrez Khan and others (PLD 1985 SC 11) and State v. Abdul Ghaffar (1996 SCMR 678).

10. On reappraisal of the record, it appears that the prosecution case was not founded upon a solitary allegation or an isolated electronic entry. It rested upon the testimony of the complainant and the victim concerning the alleged false Facebook profiles operating under the names “Maya Ali” and “Kazim Khan Shah”, the Facebook business record and registration IP address relating to the profile “Kazim Khan Shah”, the subscriber particulars supplied by the internet service provider, the mobile number linked with the respondent, the WhatsApp material extracted from the Samsung Galaxy J7 produced by the complainant and the forensic findings recorded in respect of the separately examined electronic devices. These circumstances were, therefore, required to be examined in their proper sequence and assessed cumulatively.

11. The prosecution’s oral account was furnished by complainant Major (Retd.) Mumtaz Hussain Shah and PW-07 Syeda Mehvish Ali, the victim. Their evidence explained the circumstances leading to the complaint and the production of the Samsung Galaxy J7 associated with the victim. It further described her employment with the respondent, the access he had to her personal particulars and electronic accounts, the subsequent loss of control over those accounts and the misuse of her photographs and personal information through false Facebook profiles, WhatsApp and email. Though neither witness had personally observed the technical acts of unauthorized access, installation of software or electronic transmission, their evidence identified the origin of the complaint, the victim-related material and the circumstances requiring technical verification.

12. During cross-examination, the victim admitted that she had not personally seen the respondent installing the Cerberus application and could not specify the exact date and time of every unauthorized access, transmission or upload. She also admitted that no formal complaint had been made during the subsistence of her employment and expressed uncertainty regarding the person who had recorded one of the videos referred to by her. These admissions required cautious appraisal but did not justify wholesale rejection of her evidence. Unauthorized access to an electronic account, installation of monitoring software and transmission of private data are

ordinarily acts committed in secrecy, and the victim could not reasonably be expected to witness the technical method employed. Her account was, therefore, required to be tested against the independent electronic and forensic evidence.

13. The absence of direct ocular evidence regarding the technical acts attributed to the respondent must be considered in the context of the nature of electronic offences. Such offences are ordinarily committed through information systems in a virtual environment and away from public view. Absence of conventional ocular evidence cannot, therefore, by itself be treated as fatal where the creation, access, operation or transmission of electronic material is established through reliable electronic, documentary and circumstantial evidence. Section 27 of PECA provides that an offence shall not be denied legal recognition or enforcement merely because it was committed in relation to or through the use of an information system, while Section 3 of the Electronic Transactions Ordinance, 2002 accords legal recognition and evidentiary effect to electronic records and communications. These provisions do not dispense with proof of source, identity, authenticity and integrity; however, electronic evidence cannot be discarded merely because the act was not witnessed in the conventional manner.

14. The technical evidence relating to the Facebook profile “Kazim Khan Shah” was introduced through PW-04 Inspector Tariq Arab, who deposed regarding the inquiry undertaken upon receipt of the complaint and the information obtained in relation to the said profile. He produced the initial technical report containing the particulars received in relation to the account. The Facebook business record disclosed account ID No.100025610798404, the registered email address “khankazimisb@outlook.com”, registration through IP address 196.194.131.38 on 22.04.2018 and deactivation of the account on 11.02.2019. The record produced through him established the technical particulars of the impugned profile and provided an evidentiary basis independent of the oral allegations of the complainant and the victim.

15. The account-related information brought on record by PW-04 was followed by the evidence of PW-08 Sub-Inspector Imran Saad concerning the subsequent investigation, correspondence with the relevant service providers and the documents through which the Facebook, IP and subscriber information was obtained. He produced the relevant correspondence, seizure documents and service-provider record and brought on record the information tracing IP address 196.194.131.38 to an internet connection standing in the name of Noreen Qaiser, wife of the respondent, at the Clifton premises where the respondent resided. The evidence of PW-04 and PW-08 thus supplied the independent documentary foundation connecting the

impugned Facebook profile with the respondent's household. The Facebook account information, registration IP address and subscriber particulars originated from independent service providers and were not dependent upon the credibility of the complainant or the victim alone. This evidence was required to be assessed separately from the devices recovered during the residential search, as it originated from the relevant service providers and did not depend upon the integrity of those seized devices.

16. The evidentiary value of the IP address and subscriber particulars must, however, be assessed with due caution. An IP address may identify the internet connection through which an electronic event occurred, but does not, by itself, conclusively establish the identity of the particular person who operated it. In the present case, however, the prosecution did not rely upon the IP address in isolation. Mobile No.0345-2130920 supplied an additional and more direct link. Although the number stood registered in the name of Noreen Kaiser, the respondent, while recording his statement under Section 342, Cr.P.C., himself produced his complaint dated 07.01.2017 as Mark-4. The concluding page of that complaint bears his name, residential address, CNIC number and mobile No.0345-2130920. The document emanated from the respondent himself and constituted his prior acknowledgment of the use of the said number before the commencement of the present proceedings. The connection of the respondent with the relevant mobile number, therefore, did not rest merely upon the formal subscriber particulars.

17. The forensic examination of the Samsung Galaxy J7 produced by the complainant was conducted by PW-05 Muhammad Aamir Zaib Khan, who produced his report at Exh.7/A. The device bore IMEI No.356174079821495 and was configured with WhatsApp No.+923238552798 in the name of "Mehvish". The examination disclosed a WhatsApp chat with mobile No.+923452130920 and transmission of suspected objectionable pictures from the said number to the victim's WhatsApp account. The report further recorded that the email account "s.mehvish.ali@gmail.com" was configured in the device and that the application "Cerberus", operating under the disguised name "System Framework", was installed therein. Emails, SMS messages, call logs, contacts, installed applications, web-search history and other digital data were also extracted. Since mobile No.0345-2130920 had been acknowledged by the respondent in his own complaint produced as Mark-4, the WhatsApp material supplied an electronic link between that number and the objectionable pictures transmitted to the victim's device.

18. In cross-examination, PW-05 could not identify the person who had installed the Cerberus application and did not attribute to the respondent the personal uploading of material to the pornographic website. These

admissions confined the scope of his opinion but did not affect the positive findings that the complainant-produced Samsung Galaxy J7 contained WhatsApp communication with mobile No.0345-2130920, transmission of suspected objectionable pictures from that number, the victim's configured email account and Cerberus spyware operating under the disguised name "System Framework". Since the said mobile number stood acknowledged by the respondent in Mark-4, those findings retained independent incriminating significance.

19. The evidence of PW-06 Nauman Ali is relevant only to the distinction between the electronic articles examined by him and the Samsung Galaxy J7 separately examined by PW-05. He examined the electronic articles recovered from the respondent's premises and produced his reports at Exhs.8/A and 8/B. His examination did not establish hacking of the victim's Gmail account, creation of the profile "Maya Ali" or installation of spyware in the devices examined by him. These findings, however, related to a separate set of electronic articles and did not contradict the forensic findings recorded by PW-05 in respect of the Samsung Galaxy J7 independently produced by the complainant. PW-05 examined the said device bearing IMEI No.356174079821495, whereas PW-06 examined another Samsung Galaxy J7 and other articles recovered from the respondent's premises. The learned appellate Court, therefore, was not justified in treating the findings relating to the devices examined by PW-06 as negating the WhatsApp and Cerberus material found in the separate device examined by PW-05.

20. Since the learned appellate Court placed considerable reliance upon Section 33 of PECA while assessing the electronic evidence, the relevant statutory framework may now be noticed. The material portion of Section 33 reads as follows:—

“33. Dealing with seized data or information system.—

(1) If any data or information system has been seized or secured following a search or seizure under this Act, the authorized officer who undertook the search or seizure shall, at the time of the seizure,—

- (a) make a list of what has been seized or rendered inaccessible, with the date and time of seizure; and
- (b) give a copy of that list to,—
 - (i) the occupier of the premises; or
 - (ii) the owner of the data or information system; or
 - (iii) the person from whose possession the data or information system has been seized, in a prescribed manner in the presence of two witnesses.

- (2) The authorized officer, upon an application of the owner of the data or information system or an authorized agent of the owner and on payment of prescribed costs, shall provide forensic image of the data or information system to the owner or his authorized agent within a time prescribed under this Act.”

The provision regulates the manner in which data or an information system seized or secured during a search is to be dealt with. It requires preparation of a contemporaneous list of the material seized or rendered inaccessible, specifying the date and time of seizure, and delivery of a copy thereof to the occupier, owner or person from whose possession the material was seized, in the manner prescribed by the provision. It further enables the owner or authorized agent, subject to an application and payment of the prescribed costs, to obtain a forensic image within the prescribed period. The effect of the alleged non-compliance with these requirements shall be examined in the light of the nature, source and manner of collection of the electronic evidence available in the present case.

21. In the light of the above statutory framework, the reasoning adopted by the learned appellate Court with reference to Section 33 of PECA may now be considered. The learned appellate Court observed that the articles recovered from the respondent’s premises had not been inventoried and dealt with in the prescribed manner; that independent persons had not been associated as witnesses; that the devices had not been properly sealed; that their custody and transmission had not been satisfactorily established; and that the delay in completion of the forensic reports created the possibility of manipulation. On that basis, it extended doubt to the residential recovery and the electronic evidence generally. Section 33 embodies an important safeguard concerning the inventory and traceability of seized electronic material, and its requirements cannot be treated as empty formalities. A departure from those requirements may affect the weight and reliability of the particular article concerned. The provision, however, does not expressly declare that every procedural irregularity automatically renders the seizure void or excludes all evidence subsequently obtained. The learned appellate Court was, therefore, required to identify the precise lapse, the particular device affected and the manner in which such lapse created a real doubt regarding its identity, substitution, alteration or the integrity of the data extracted therefrom. Investigative deficiencies may justify cautious scrutiny, but an abstract possibility of tampering cannot, without supporting evidence, be treated as proof that substitution, alteration or fabrication actually occurred.

22. The record contains the seizure memo and the forensic reports describing the evidentiary articles, their receipt particulars, evidence labels and identifying features. The learned appellate Court did not identify any

particular relevant device whose IMEI number, serial number, evidence label or other identifying particular materially differed from the article received and examined by the forensic laboratory. The non-production of the search warrant or departure entry, non-association of private witnesses, failure immediately to seal every device and delay in completion of the detailed forensic reports were matters requiring cautious scrutiny and could affect the weight attached to the residential recovery. They could not, without evidence of actual substitution, alteration or misidentification, be treated as affirmative proof that the relevant devices or extracted data had been fabricated.

23. More importantly, the alleged irregularities concerning the residential search could not affect every part of the prosecution evidence. The Facebook account information, registration IP address, IP logs and subscriber particulars were independently supplied by the relevant service providers and were not extracted from the devices recovered from the respondent's premises. The Samsung Galaxy J7 examined by PW-05 under Exh.7/A had also been separately produced by the complainant and forwarded for forensic examination through a distinct production and seizure process. Any defect relating to the inventory, sealing, custody or handling of the devices recovered during the residential search had to be confined to those particular articles. By extending that objection to the independent service-provider record and the separately produced Samsung Galaxy J7, the learned appellate Court allowed an objection concerning one part of the investigation to overshadow distinct and independently sourced electronic evidence.

24. The learned appellate Court considered the internet connection and mobile number mainly with reference to their formal registration in the name of the respondent's wife. It did not distinguish between nominal registration and actual use. The evidence showed not merely that the registered subscriber was related to the respondent, but that the relevant internet connection was installed at his residence, that he had himself acknowledged the use of mobile No.0345-2130920 in Mark-4 and that the same number appeared in the victim-associated Samsung Galaxy J7 as the source of suspected objectionable pictures. These circumstances were interlocking and could not properly be evaluated as unrelated coincidences.

25. The respondent examined DW-01 Mehmood Ahmed Malik, a questioned-document expert, who expressed opinion under Exhs.13/A and 13/B regarding the signatures appearing on two documents connected with production and forwarding of the complainant-produced mobile phone. Even if his opinion is accepted at its highest, it raises a question only regarding the signatures appearing on those documents. It neither identifies the person

who wrote the questioned signatures nor establishes that the Samsung Galaxy J7 was substituted, that its internal contents were fabricated or that the Facebook, IP and mobile-number records were false. The opinion of an expert is relevant but advisory and could not be extended beyond the signatures and documents actually examined by him.

26. The victim's statement that she had not personally handed over the mobile phone to the FIA was also treated as contradicting the prosecution case. The complainant stated that he had voluntarily produced the phone on behalf of his daughter, while the internal contents of the device corresponded with her configured WhatsApp number, email account and personal communications. Her failure personally to deliver the phone did not establish that the device had not been produced or that the Samsung Galaxy J7 examined under Exh.7/A was unrelated to her. The evidence concerning its production, forwarding and internal identifying data had to be considered as a whole rather than upon an isolated answer elicited during cross-examination.

27. The learned appellate Court also assigned undue significance to the objection concerning the examination of the respondent under Section 342, Cr.P.C. The record reflects that he was confronted with the substance of the prosecution case relating to the false Facebook profiles, relevant electronic accounts and mobile numbers, objectionable electronic material, recovery of devices and forensic evidence, and was afforded an adequate opportunity to offer his explanation. The law does not require every line or technical expression appearing in a forensic report to be reproduced verbatim in the statement under Section 342, Cr.P.C. No subsidiary technical entry not brought to his notice is being treated as the sole basis for maintaining the conviction. The objection, therefore, did not justify rejection of the electronic and documentary circumstances brought on record.

28. In a case based upon electronic and circumstantial evidence, each circumstance need not independently establish the entire charge; its probative value lies in its connection with the other proved circumstances. An IP address, viewed separately, may identify only the internet connection through which an electronic event occurred; subscriber particulars may identify the registered subscriber; and a forensic entry may establish the existence of a communication, application or item of data. Such circumstances are, therefore, required to be assessed collectively to determine whether they form a coherent and reliable chain connecting the accused with the alleged electronic activity.

29. The learned appellate Court did not merely adopt another reasonably possible view of the evidence. It assessed the prosecution material in

isolation and failed to appreciate the manner in which the different circumstances supported one another. The absence of relevant data in some of the devices examined by PW-06 was treated as undermining the distinct findings recorded by PW-05 in respect of the Samsung Galaxy J7 separately produced by the complainant. Likewise, the alleged non-compliance with Section 33 of PECA was extended beyond the devices recovered from the respondent's residence and was used to discredit electronic material independently obtained from the service providers and from the separately produced mobile phone. The opinion of the defence questioned-document expert was also assigned a scope wider than the limited question of the disputed signatures examined by him. When the evidence is viewed in its proper sequence and cumulative effect, the profile "Kazim Khan Shah" stands connected with the IP address assigned to the internet connection installed at the respondent's residence. Mobile No.0345-2130920 is independently linked with the respondent through his own complaint produced as Mark-4, while the same number appears in the Samsung Galaxy J7 associated with the victim as the source from which suspected objectionable pictures were transmitted to her WhatsApp account. The presence of Cerberus spyware in that device provides an additional corroborative circumstance concerning electronic monitoring, although its installer could not independently be identified. These circumstances originated from separate sources and, when considered together, establish the respondent's connection with the offending electronic activity beyond reasonable doubt. The nature and purpose of the proved conduct further disclose the requisite dishonest and harmful intention. The impugned judgment, therefore, suffers from material misreading and non-reading of the evidence and cannot be sustained.

30. For the foregoing reasons, the instant criminal acquittal appeal is allowed; the impugned judgment dated 22.05.2025, passed by the learned Sessions Judge, Karachi South, is set aside; and the judgment of conviction and sentence dated 08.05.2024, passed by the learned Civil Judge and Judicial Magistrate-I, Karachi South, is restored. The respondent shall be taken into custody to undergo the sentences awarded to him, with the benefit of Section 382-B, Cr.P.C., as extended by the learned trial Court.

JUDGE