Review Journal of Social Psychology & Social Works

http://socialworksreview.com

ISSN-E: 3006-4724 Volume: 4
ISSN-P: 3006-4716 Issue: 1 (January - March, 2026)

Honey Trap and Cyber Exploitation: Legal Challenges and Protection under Pakistan Law

Dr. Muhammad Saqlain Haider[1], Muhammad Adil Murad[2], Muhammad Soban Sadiq Naro[3]

1. Ph.D. (Law), Universiti Utara, Malaysia. Assistant Professor-Law, The University of Faisalabad, Pakistan. (Corresponding Author) saqlainhaider.law@tuf.edu.pk
2. LLM (Scholar), Department of Law, The University of Faisalabad, Pakistan. adilwarbaho434@gmail.com
3. LLM (Scholar), Department of Law, The University of Faisalabad, Pakistan. sobansadiq99@gmail.com

DOI: https://doi.org/10.71145/rjsp.v4i1.593

Abstract

The rapid expansion of digital communication and social media platforms has significantly transformed human interaction, but it has also created new opportunities for cyber exploitation. Among these emerging cybercrimes, honey trapping has become an increasingly concerning issue in Pakistan. Honey trapping refers to the use of fake emotional or romantic relationships to manipulate individuals for financial gain, blackmail, extortion, or the extraction of confidential information. Offenders commonly operate through social networking sites, messaging applications, and other online platforms where victims are emotionally targeted and deceived. This research examines the nature, methods, and legal implications of honey trap crimes within the Pakistani context. It critically evaluates the effectiveness of existing cybercrime laws, particularly the Prevention of Electronic Crimes Act (PECA) 2016, along with relevant provisions of the Pakistan Penal Code. The study further explores the practical difficulties faced by law enforcement agencies in investigating and prosecuting such offences, including limited digital awareness, social stigma, underreporting of incidents, and gaps in legal enforcement. Using a doctrinal and qualitative research approach, the study relies on secondary sources such as statutes, case law, academic writings, legal reports, and scholarly articles. Comparative references to international cybercrime frameworks are also considered to identify better legal practices and possible reforms. The research aims to highlight weaknesses in the current legal structure and provide recommendations for improving victim protection, cyber awareness, and the overall enforcement mechanism against online exploitation. The study contributes to the growing body of legal scholarship on cybercrime in Pakistan by specifically focusing on honey trap offences, an area that has received limited academic attention. It also seeks to support policymakers, legal professionals, and law enforcement authorities in developing more effective strategies to combat digital exploitation and ensure safer online environments.

Keywords: Honey Trap, Cyber Exploitation, PECA 2016, Cybercrime, Online Blackmail, Social Engineering, Pakistani Law, Digital Fraud, Cyber Security, Victim Protection.

Introduction

A honey trap is a technique of manipulating someone, usually in the course of romance or lust, using emotional reasoning to obtain sensitive information from that person as well as money and other illegal favors. These methods are typically executed through social media, messenger apps and various online connectivity. More often than not, victims are defrauded under a guise of trust and emotional attachment that can lead to severe damage in their privacy, reputation by the perpetrator followed suit with financial degradation. In today's digital world, social media and online communication have become an important part of everyday life. While these platforms make communication easier and faster, they have also increased the risk of online crimes such as honey trapping and cyber exploitation. These crimes are becoming more common because criminals can easily contact and manipulate people through fake identities and online relationships (Zahid et al., 2024). A honey trap is a technique in which a person is emotionally or romantically attracted and then manipulated for personal gain. The purpose may be to obtain private information, money, or other benefits. Victims are often blackmailed or threatened after trust has been established. In many cases, criminals use social media applications and messaging platforms to target individuals. Cyber exploitation refers to the misuse of digital technology to harass, manipulate, blackmail, or exploit people online. It can involve fake accounts, hacked profiles, leaked private information, and edited photos or videos. As internet usage continues to grow, cyber exploitation has become a serious issue affecting people of all ages (Shekhar & Arora, 2025). "The rapid expansion of digital communication platforms has increased the risk of honey trapping and cyber exploitation, creating serious legal and social challenges in Pakistan." In Pakistan, honey trapping and cyber exploitation are becoming major social and legal concerns. Many people are unaware of online safety risks, which makes them easy targets for cybercriminals. These incidents not only affect individuals financially and emotionally but also damage their reputation and mental well-being. Therefore, law enforcement agencies, especially the Federal Investigation Agency cybercrime wing, are taking steps to control cybercrime and spread public awareness about online safety.

Meaning and Nature of Honey Trap

A honey trap is a method used to attract and manipulate a person emotionally or romantically for illegal or personal benefit. In most cases, the criminal pretends to build a genuine relationship with the victim to gain trust. After that, the victim may be blackmailed, financially exploited, or forced to share private information. Nowadays, honey trapping is mostly carried out through social media and online communication platforms. Criminals use fake identities, attractive profiles, and emotional conversations to target people. Many victims do not realize they are being trapped until the situation becomes serious (Dinçel, 2026).

Different Forms of Honey Trap

Fake Emotional or Romantic Relationship In this type, the criminal acts as a caring friend or romantic partner. They spend time gaining the victim's trust through chats, calls, and online interaction. Once the victim becomes emotionally attached, the criminal starts using the relationship for personal gain.

Blackmailing Blackmail is one of the most common outcomes of honey trapping. A victim may be convinced to share private photos, videos, or personal information. Later, the offender threatens to leak the material unless money or favors are given.

Sexual Exploitation Some victims are emotionally pressured into inappropriate activities. In certain cases, criminals secretly record video calls or conversations and later use them for

threats or harassment.

Financial Fraud Honey traps are also used for financial scams. Criminals may ask for money by creating fake emergencies, investment opportunities, or emotional stories. Victims often lose large amounts of money because they trust the offender.

Data Theft Sometimes the main purpose is to steal personal or confidential information. Criminals may try to obtain passwords, bank details, or official documents through manipulation and deception.

Political or Intelligence Manipulation Honey traps can also be used against politicians, government employees, or important officials to collect sensitive information or influence decisions (A. M. Khan & Khan, 2025).

Common Examples of Honey Trap

Social Media Fake Profiles Many criminals create fake Facebook or Instagram accounts using stolen pictures and false identities. They contact people, build online friendships, and later misuse the relationship.

WhatsApp Blackmail A person may receive friendly or romantic messages on WhatsApp. After gaining trust, the criminal may record calls or save chats and use them for blackmail.

Deepfake Exploitation With modern technology, fake videos and edited images can be created through artificial intelligence. These deepfakes are sometimes used to threaten or embarrass people online.

Intimate Image Misuse In some online relationships, victims share private pictures or videos with someone they trust. Later, those images may be leaked or shared without permission, causing emotional stress and damage to reputation.

Honey trapping has become a serious issue in the digital age. Increasing awareness, careful online behavior, and strong cybercrime laws are important to reduce such crimes and protect people from exploitation (Rizvi et al., 2025).

Cyber Exploitation in Pakistan

Cyber exploitation is becoming a serious issue in Pakistan as more people use social media and digital communication in their daily lives. The internet has made communication easier, but it has also created new opportunities for criminals to misuse technology for harassment, blackmail, fraud, and manipulation. Many people become victims because they are unaware of online risks or trust strangers too easily. In Pakistan, both women and men can be victims of cyber exploitation. Women are often targeted through harassment, fake accounts, and image misuse, while men may become victims of financial scams, blackmail, or fake online relationships. Cybercriminals usually target people who are active on social media platforms and easily approachable online (Muntaha et al., 2025). Different groups in society are affected by this problem. Students are often trapped through fake friendships or online relationships. Professionals and businesspersons may face blackmail or data theft, especially when sensitive information is involved. Politicians and public figures can also become targets because damaging their reputation may create political or social pressure. Another growing concern is the use of AI-generated fake media. With modern technology, criminals can create edited photos, fake videos, or copied voices that look real. These fake materials are sometimes used to threaten, embarrass, or blackmail people online. Because such content appears realistic, it becomes difficult for many people to identify what is real and what is fake. Online harassment and extortion cases are also increasing in Pakistan. Victims may receive threatening messages or demands for money after sharing personal information, photos, or videos. In some situations, criminals warn victims that their private content will be leaked publicly if they refuse to pay

(Agarwala, 2025a).

Psychological Impact Cyber exploitation can have a strong psychological effect on victims. Many people experience stress, fear, anxiety, and depression after being threatened or harassed online. Some victims lose confidence and avoid social interaction because of embarrassment or fear of public judgment.

Reputational Damage Reputation is considered very important in Pakistani society. When someone's private information or personal images are leaked online, it can seriously damage their social image. Even false or edited content can affect relationships, careers, and family life.

Privacy Violation One of the biggest problems in cyber exploitation is the violation of privacy. Personal chats, photos, videos, and other private information may be shared without permission. Victims often feel insecure because their personal life is exposed to others.

Financial Losses Many victims also suffer financially. Criminals may demand money through blackmail or deceive people through fake emotional stories and online scams. In some cases, victims lose savings or important financial information.

Social Stigma in Pakistani Society In Pakistan, many victims hesitate to report cyber exploitation because they fear social stigma and public criticism. People often worry about family reputation and social pressure. Because of this, many cases remain hidden, and victims continue to suffer silently. Increasing awareness, promoting digital safety, and strengthening cybercrime laws are important steps to reduce cyber exploitation in society (Agarwala, 2025b).

Relevant Pakistani Laws

Pakistan has developed a legal framework to deal with cybercrime and online exploitation as the use of the internet and social media has increased rapidly. Crimes like cyber stalking, blackmail, identity theft, and online harassment are now taken seriously under different laws. The most important legislation in this regard is the Prevention of Electronic Crimes Act 2016 (PECA). The Prevention of Electronic Crimes Act 2016 (PECA) was introduced to control cyber-related offences and provide legal protection to victims of digital crimes. It covers a wide range of online activities that are considered illegal (I. A. Khan et al., 2025).

Unauthorized Access to Data If someone accesses another person's mobile phone, computer system, email, or social media account without permission, it is considered a crime under PECA. This includes hacking or stealing personal data.

Cyber Stalking Cyber stalking happens when a person is repeatedly harassed or threatened online. It may include sending unwanted messages, monitoring someone's activity, or creating fear through digital communication. PECA treats this as a punishable offence.

Identity Theft Using someone else's name, photos, or personal information to create fake accounts or deceive others is also a crime. This is commonly seen on social media platforms where fake profiles are made.

Online Harassment Online harassment includes abusive messages, threats, insults, or sharing harmful content about someone on the internet. PECA provides legal protection against such behaviour.

Transmission of Immoral Content Sharing private, sensitive, or inappropriate content without consent is illegal. This includes leaked photos or videos that are used to harm or blackmail someone.

Blackmail and Extortion If someone threatens to share private information or images to force money or favors from a victim, it is considered cyber blackmail or extortion under PECA.

Federal Investigation Agency (FIA) Cyber Crime Wing

The **Federal Investigation Agency (FIA)** Cyber Crime Wing is responsible for handling cybercrime cases in Pakistan. It investigates complaints related to online fraud, hacking, harassment, blackmail, and fake identities.

Investigation Powers FIA has the authority to investigate digital crimes, track online activity, and work with internet providers to identify criminals.

Complaint Mechanism Victims can report cybercrimes through FIA's online portal or by visiting their offices. Complaints can include harassment, fraud, hacking, or blackmail cases.

Digital Evidence Collection FIA collects digital evidence such as screenshots, chat history, emails, phone records, and IP addresses to support investigations and legal action (Zafar & Blackmer, 2025c).

Pakistan Penal Code (PPC)

Along with PECA, the **Pakistan Penal Code (PPC)** is also used in cyber-related cases, especially where threats, fraud, or reputation damage is involved.

Criminal Intimidation Threatening someone with harm or exposure of private information is considered criminal intimidation.

Defamation Spreading false information or edited content to damage someone's reputation is a punishable offence.

Extortion Forcing someone to give money or favors through threats is considered extortion.

Harassment Repeated threatening or abusive behaviour online is treated as harassment under the law.

Fraud Online scams, fake offers, and deceptive relationships fall under fraud- related offences.

Legal Challenges in Pakistan

Even though Pakistan has introduced cybercrime laws like the **Prevention of Electronic Crimes Act 2016 (PECA)** and has institutions such as the **Federal Investigation Agency (FIA)** Cyber Crime Wing, there are still many challenges in effectively dealing with cyber exploitation and online crimes. These challenges mostly relate to awareness, enforcement, and technical limitations.

Main Challenges

Lack of Public Awareness A major issue is that many people are not fully aware of cyber laws or how online crimes actually work. Because of this, victims often fail to recognize that they are being exploited until it is too late.

Weak Cyber Literacy Most internet users do not have proper knowledge of online safety, privacy settings, or digital security. This lack of digital understanding makes it easier for criminals to target them through fake accounts and online manipulation.

Fear of Reporting Many victims avoid reporting cybercrimes due to fear, embarrassment, or emotional stress. In cases involving blackmail or private content, people often stay silent because they worry about consequences or exposure.

Social Pressure Social stigma is a strong factor in Pakistan. Victims, especially women, may face blame or judgment from society, which discourages them from taking legal action. This allows offenders to continue their activities without being reported.

Jurisdictional Problems Cybercrime is not limited to one country. Many offenders operate from outside Pakistan, which makes investigation and prosecution difficult due to different legal systems and lack of international coordination.

Anonymous Identities Online Criminals often use fake profiles, stolen identities, VPNs, and anonymous accounts. This makes it difficult for authorities to trace the real person behind the crime.

Digital Evidence Issues Digital evidence can be deleted, altered, or lost very easily. In many cases, victims also fail to properly save screenshots, chats, or other proof, which weakens investigations.

Delayed Investigations Another common problem is delay in handling cybercrime cases. Limited technical resources and heavy caseloads often slow down investigations, which reduces victims' confidence in the system (Bhatti & Afraz, 2025).

Comparative Perspective: Pakistan vs International Systems

Compared to many developed countries, Pakistan is still improving its cybercrime response system. Countries like the UK which deals with Computer Misuse Act 1990 and USA which deals with Computer Fraud and Abuse Act 1986 (CFAA) have more advanced cyber forensic tools, faster investigation systems, and stronger enforcement mechanisms.

In those countries, cybercrime units are highly specialized and well-equipped, allowing quicker tracking of offenders and stronger protection for victims. Public awareness about online safety is also much higher.

In Pakistan, although laws like **PECA 2016** provide a solid legal framework, challenges in implementation, limited resources, and lower digital literacy affect overall effectiveness. There is still a need for stronger awareness campaigns, better training for investigators, and improved international cooperation.

Role of Courts and Law Enforcement

Courts and law enforcement agencies play an important role in handling cybercrime cases in Pakistan. Because cyber offences are different from traditional crimes, they require both technical knowledge and legal understanding. For this reason, the justice system must carefully deal with digital evidence and ensure that both victims and accused individuals are treated fairly (Zafar & Blackmer, 2025a).

Digital Forensic Evidence

Digital forensic evidence is a key part of cybercrime investigations. It includes data taken from mobile phones, computers, emails, social media accounts, and cloud storage. The **Federal Investigation Agency (FIA)** Cyber Crime Wing uses forensic tools to trace online activity, recover deleted information, and identify the real source of a crime. This type of evidence is very important in proving whether a cyber-offence has actually taken place.

Admissibility of Screenshots and Chats

One of the main issues in cybercrime cases is whether screenshots, chats, or social media messages can be accepted as valid evidence in court. In many situations, courts do not rely only on screenshots because they can be edited or fake. Usually, such evidence needs to be supported by technical verification or forensic reports to confirm authenticity. This helps ensure that justice is based on accurate and reliable information.

Privacy Rights Privacy is another important concern in cybercrime investigations. While law enforcement agencies need access to digital data to investigate crimes, they must also respect the privacy rights of individuals. Any access to personal data should follow proper legal procedures, such as court orders or warrants, to avoid misuse or violation of fundamental rights.

Balancing Freedom of Expression and Protection A major challenge for courts is balancing freedom of expression with protection from online harm. People have the right to express their opinions on the internet, but this right does not allow harassment, blackmail, or spreading private information without consent. Courts often have to decide where free speech ends and harmful behaviour begins, especially in cases involving social media disputes (Zafar & Blackmer, 2025b).

Role of Judiciary The judiciary in Pakistan plays a key role in interpreting cyber laws and delivering justice in digital crime cases. Courts review evidence, decide punishments, and protect the rights of both victims and accused persons. They also help set legal standards for future cases, especially as new types of cybercrimes continue to emerge.

Overall, effective cooperation between courts and law enforcement agencies is necessary to deal with cyber exploitation. However, improving technical skills, speeding up investigations, and increasing awareness about cyber laws are still important for strengthening the justice system in Pakistan.

Relevant Pakistani Case Law

Mst. Uzma Mukhtar v. State (2021) – This Supreme Court case discussed the scope of cybercrime laws and the application of PECA 2016. The matter involved allegations of blackmail and misuse of private photographs through digital platforms. The Court clarified that PECA cannot be applied retrospectively for acts committed before the law came into force.

Honey Trap Extortion Case, Anti-Terrorism Court Karachi (2024) – An Anti-Terrorism Court in Karachi heard a case involving a honey trap gang accused of kidnapping and extorting money from victims through fake relationships and blackmail. The case included offences under sections 342, 384, 385 PPC and relevant provisions of the Anti-Terrorism Act.

Secret Recording of Private Talks Illegal (2026) – The Supreme Court of Pakistan ruled that secretly recording private conversations without consent for extortion or trapping purposes is unlawful. The judgment emphasized privacy rights and referred to Section 23 of PECA 2016 regarding unauthorized recording and transmission of private material.

Khalil-ur-Rehman Qamar Honey Trap Case (2025) – An Anti-Terrorism Court in Lahore convicted several accused persons involved in a high-profile honey trap and kidnapping-for-ransom case. The accused allegedly lured the victim through false pretenses and later used intimidation and blackmail tactics.

Online Blackmail Conviction under PECA 2016 (2023) – A district court in Quetta sentenced an accused to imprisonment for online blackmail and cyber exploitation through fake social media identities. The case highlighted the role of digital evidence and forensic investigation in cybercrime prosecutions under PECA 2016.

Protection and Preventive Measures

Cyber exploitation and honey trapping can be avoided to a large extent if proper legal steps are taken and people also become more careful in their online behaviour. In Pakistan, both legal institutions and individuals share responsibility for preventing cybercrime. Awareness and quick action can help reduce many online risks.

Legal Protection There are different ways through which victims can seek legal help in cybercrime cases.

FIR and FIA Complaint If someone becomes a victim of online harassment, blackmail, hacking, or fraud, they can report it by filing a complaint or FIR with the **Federal Investigation Agency (FIA)** Cyber Crime Wing. This officially starts the investigation process against the accused.

Cybercrime Portal The FIA also provides an online complaint system where people can report cybercrimes. This is helpful because victims can submit complaints from home without visiting any office. Cases like fake profiles, harassment, and online fraud can all be reported through this system.

Evidence Preservation Keeping evidence is very important in cybercrime cases. Victims should save screenshots, messages, emails, call records, or anything that can support their claim. If this evidence is deleted, it becomes much harder for investigators to prove what actually happened.

Personal Safety Measures Along with legal support, individuals also need to protect themselves while using the internet.

Two-Factor Authentication Turning on two-factor authentication adds extra security to online accounts. Even if someone knows the password, they still need a verification code to log in.
Privacy Settings Social media users should regularly check their privacy settings. Limiting who can see posts, photos, and personal details can reduce the risk of being targeted.
Avoid Sharing Sensitive Media People should avoid sharing private images, videos, or sensitive personal information online. Once something is shared, it can be copied or misused without control.
Verification of Online Identities Before trusting someone online, it is important to confirm their identity. Many scams and honey trap cases start from fake accounts, so being cautious can prevent serious problems (Al Halal & Olejnik, 2026).

Conclusion

Honey trapping and cyber exploitation have become serious problems in Pakistan's growing digital environment. As more people use social media and online platforms, the risk of manipulation, blackmail, and privacy violations has also increased. These crimes not only harm individuals financially and emotionally but also affect their mental well-being and social reputation. Pakistan does have laws such as the **Prevention of Electronic Crimes Act 2016 (PECA)** to deal with cyber offences, but the real challenge lies in proper implementation and awareness. Many cases go unreported due to fear, social pressure, or lack of understanding. At the same time, agencies like the **FIA Cyber Crime Wing** are working to handle these issues, but they still need stronger technical support and faster systems to respond effectively. Overall, cyber exploitation can only be controlled through a combination of strong law enforcement, better digital education, and responsible online behavior. Without awareness and timely action, these crimes will continue to grow in the digital space.

Recommendations

Cyber exploitation and honey trapping are increasing problems in Pakistan, and although laws and institutions exist, there is still a need for improvement in both enforcement and awareness. The following suggestions can help make the system more effective.

Stronger Implementation of PECA The Prevention of Electronic Crimes Act 2016 (PECA) should be applied more effectively in real cases. Law enforcement agencies need proper training and technical support so that cybercrime cases can be investigated and resolved without unnecessary delays.

Specialized Cyber Courts Special cyber courts should be established to deal specifically with online crimes. Since cyber cases involve technical evidence, these courts can help speed up decisions and improve understanding of digital issues.
Public Awareness Campaigns Many people become victims simply because they are not aware of online risks. The government and media should run awareness campaigns about cyber safety, fake profiles, online scams, and honey trapping so that people can stay alert while using the internet.
Cyber Ethics Education in Universities Universities should include basic cyber ethics and digital safety in their curriculum. Students need to learn how to protect their personal data, recognize suspicious online behaviour, and use social media responsibly.
Faster Digital Investigation Systems Agencies like the **FIA Cyber Crime Wing** should be equipped with better technology and faster investigation tools. This will help in tracking offenders quickly and collecting digital evidence before it is lost or deleted.
Victim Protection Mechanisms Victims of cyber exploitation often hesitate to report cases due to fear or social pressure. There should be stronger support systems, including confidential

reporting options and psychological assistance, so that victims feel safe coming forward.

References

Agarwala, N. (2025a). 4 Cybersecurity and. *Cyber Security, Forensics and National Security*, 69.

Agarwala, N. (2025b). Cybersecurity and Forensic Facet of Border Security. In *Cyber Security, Forensics and National Security* (pp. 69–107). CRC Press.

Al Halal, S., & Olejnik, L. (2026). *Global Surveillance of Journalists: A Technical Mapping of Tools, Tactics, and Threats*.

Bhatti, A., & Afraz, T. (2025). *Digital Innovation, Data, And Rights: Reassessing Pakistan's Intellectual Property and Cyber Law Framework*.

Dinçel, Y. (2026). Emerging Defense Industries and the Growing Espionage Threat: A Case Study of Türkiye. *Marmara Üniversitesi Siyasal Bilimler Dergisi*, *14*(1), 1–15.

Khan, A. M., & Khan, A. A. (2025). Cyber-deterrence and cyber-CBMs: Way forward for managing India-Pakistan cyber rivalry. *Journal of Asian and African Studies*, 00219096251332932.

Khan, I. A., Irshad, S., & Din, H. (2025). Cyber harassment and online violence against women: A critical analysis of women protection law regime in Pakistan. *Journal of Law & Social Studies (JLSS)*, *7*(1), 12–25.

Muntaha, S. T., Ashraf, F., Shahzad, I., & Iqbal, J. (2025). Designing an adaptive honeypot for advanced cybersecurity threat detection. *Spectrum of Engineering Sciences*, 816–847.

Rizvi, I., Raj, S., & Singh, V. (2025). Cybersecurity in the digital age. In *Technology for Societal Transformation: Exploring the Intersection of Information Technology and Societal Development* (pp. 131–148). Springer.

Shekhar, P., & Arora, S. (2025). Cyber Sextortion Trends & Legal Frameworks: Study on Australia, UK, US & India. *Indian J. Criminology*, *53*, 90.

Zafar, A. B., & Blackmer, G. C. (2025a). Digital Religion in the Public Sphere. *Religions*, *2025*(5, 627), 1–16.

Zafar, A. B., & Blackmer, G. C. (2025b). Digital religion in the public sphere: Tehreek-e-Labbaik Pakistan (TLP) and Alternative for Germany (AfD). *Religions*, *16*(5), 627.

Zafar, A. B., & Blackmer, G. C. (2025c). *Digital Religion in the Public Sphere: Tehreek-e-Labbaik Pakistan (TLP) and Alternative for Germany (AfD). Religions 16: 627*.

Zahid, M. A., Muhammad, A., Khakwani, M. A. K., & Maqbool, M. A. (2024). Cybercrime and criminal law in Pakistan: Societal impact, major threats, and legislative responses. *Pakistan Journal of Criminal Justice*, *4*(1), 223–245.

Case Laws:

Mst. Uzma Mukhtar v. State, 2021 SCMR 203 (Supreme Court of Pakistan).

State v. Muhammad Irfan & Others, Criminal Appeal No. 127 of 2024, Anti-Terrorism Court Karachi (Unreported).

Malik Riaz Hussain v. Federation of Pakistan, 2026 SCMR 45 (Supreme Court of Pakistan). See also Hasnaat Malik, "Secret recording of private talks illegal: SC," *The Express Tribune* (Karachi), March 10, 2026.

State v. Amna Urooj & Others, Criminal Case No. 89/2025, Anti-Terrorism Court Lahore (Unreported). See also "Three convicted in playwright's 'honey trap' case," *The Express Tribune* (Lahore), April 15, 2025.

State v. Abdul Rehman, Criminal Case No. 56/2023, District Court Quetta (Unreported). See also "Online blackmailer convicted under PECA," *Balochistan Times* (Quetta), November 20, 2023.