MONOGRAPH

Cyber Law in Pakistan: A Legal Analysis of Online Fraud, Digital Financial Crime, and Comparative International Frameworks

Abstract

The proliferation of digital technology in Pakistan has brought with it an alarming surge in cybercrime, particularly online financial fraud. This monograph critically examines the phenomenon of online fraud in Pakistan, with particular focus on WhatsApp account hacking and subsequent unauthorized money transfers via mobile wallets such as Easypaisa and JazzCash. The study maps the dominant modes of digital fraud, evaluates the adequacy of Pakistan's existing cyber law framework — primarily the Prevention of Electronic Crimes Act 2016 (PECA 2016) — and undertakes a comparative analysis with international legal instruments including the Budapest Convention on Cybercrime, the European Union's General Data Protection Regulation (GDPR), and the legal frameworks of the United Kingdom and India. The monograph concludes that while Pakistan possesses a foundational cyber law architecture, significant gaps persist in enforcement, digital forensics, and harmonization with global standards (Ali & Hasan, 2021; Federal Investigation Agency [FIA], 2023).

1. Introduction

The digital revolution has fundamentally transformed the way individuals communicate, transact, and interact. In Pakistan, the rapid expansion of mobile internet penetration — reaching over 124 million broadband subscribers by 2023 — has simultaneously created an expansive attack surface for cybercriminals (Pakistan Telecommunication Authority [PTA], 2023). Online fraud,

once a peripheral concern, has emerged as one of the most pressing sociolegal challenges confronting the Pakistani state and its citizenry.

Among the most insidious forms of cybercrime is the hacking of social media accounts — particularly WhatsApp — followed by the exploitation of victim contacts to transfer funds to anonymous mobile wallet accounts such as Easypaisa. This form of digital fraud combines social engineering, identity theft, and financial crime into a single, devastatingly effective attack vector. The Federal Investigation Agency (FIA) Cybercrime Wing reported a **47% increase** in cybercrime complaints between 2021 and 2023, with financial fraud constituting the largest category (FIA, 2023).

This monograph undertakes a comprehensive legal analysis of these phenomena, evaluating the strength and limitations of Pakistan's legal responses while drawing instructive comparisons from leading international jurisdictions. The central argument advanced is that while PECA 2016 provides a statutory foundation, its effective implementation is critically undermined by institutional deficiencies, limited digital forensic capacity, and the absence of a robust data protection regime (Cheema, 2019).

2. Modes of Online Fraud in Pakistan

Online fraud in Pakistan manifests in diverse and evolving forms. Understanding these modes is a prerequisite to any meaningful legal analysis. The following subsections detail the most prevalent typologies.

2.1 WhatsApp Account Hacking

WhatsApp account hacking represents one of the most prevalent and damaging forms of cybercrime in Pakistan. The typical attack vector involves *SIM swap fraud*, where an attacker contacts a mobile network operator posing as the legitimate account holder, requests a SIM replacement, and thereby gains control of the victim's phone number. Once the new SIM is activated, the attacker intercepts WhatsApp's one-time password (OTP) verification code and hijacks the account (Hussain & Khan, 2022).

Alternatively, attackers employ phishing messages — typically disguised as WhatsApp verification alerts or prize notifications — to trick users into revealing their OTP. A third method

involves the exploitation of WhatsApp Web sessions left open on shared or public computers. In each scenario, once account access is obtained, the fraudster impersonates the victim and solicits funds from contacts under fabricated emergency pretexts, directing payments to untraceable Easypaisa or JazzCash wallet numbers (Hussain & Khan, 2022; PTA, 2023).

2.2 Mobile Wallet Fraud: Easypaisa and JazzCash

Pakistan's mobile financial services sector, led by Easypaisa (Telenor Microfinance Bank) and JazzCash, has democratized financial inclusion, bringing banking services to millions of unbanked citizens. However, these platforms have also become conduits for financial crime. The pseudo-anonymity of mobile wallets — registered using CNICs that may be fraudulently obtained — enables criminals to receive stolen funds with relative impunity (State Bank of Pakistan [SBP], 2022).

Common fraud mechanisms include:

- Impersonation of telecom representatives to obtain wallet PINs via vishing (voice phishing) calls;
- Creation of fraudulent wallet accounts using counterfeit or stolen Computerized National Identity Cards (CNICs);
- Use of WhatsApp-hijacked accounts to solicit emergency transfers directly into fraudster-controlled wallets;
- Exploitation of inter-bank transfer loopholes and RAAST instant payment system vulnerabilities.

The State Bank of Pakistan (2022) documented over PKR 2.1 billion lost through mobile wallet fraud in fiscal year 2021–22, representing a 63% increase over the preceding year.

2.3 Phishing and Spear Phishing

Phishing attacks in Pakistan have grown in sophistication, increasingly employing spear phishing — targeted attacks crafted using personal information harvested from social media or data breaches — to deceive high-value targets including business executives and government officials. Fraudulent emails replicating official bank communications, tax notices from the Federal Board of Revenue (FBR), and NADRA correspondence have been widely documented (Cheema, 2019; FIA, 2023).

2.4 Online Banking Fraud

Unauthorized access to internet banking portals through credential theft, man-in-the-browser attacks, and malware installation constitutes another significant category of online fraud. In several documented cases, malware distributed through WhatsApp forward messages captured banking credentials and enabled fraudulent transactions without the victim's knowledge (Ali & Hasan, 2021).

2.5 Investment and Advance-Fee Fraud

Pakistan has witnessed a proliferation of fraudulent investment schemes — often promoted through Facebook groups, WhatsApp broadcasts, and YouTube channels — promising extraordinary returns. Advance-fee fraud, colloquially known as the "419 scam," remains prevalent, targeting victims with promises of lottery winnings, inheritance transfers, or business partnerships contingent on upfront payments (FIA, 2023).

2.6 E-Commerce and Classified Advertisement Fraud

Platforms such as OLX Pakistan have become vectors for purchase fraud, whereby sellers receive fake payment screenshots or buyers pay for goods that are never delivered. The absence of robust escrow mechanisms and inadequate seller verification frameworks have exacerbated this problem (PTA, 2023).

3. Pakistani Legal Framework Governing Online Fraud

3.1 Prevention of Electronic Crimes Act 2016 (PECA 2016)

PECA 2016 constitutes the primary legislative instrument governing cybercrime in Pakistan. Enacted after nearly a decade of legislative deliberation, it criminalizes a broad spectrum of digital offences and vests investigative authority in the FIA Cybercrime Wing (Government of Pakistan, 2016).

The following provisions are directly applicable to online fraud:

- **Section 14 — Identity Crime:** Criminalizes the impersonation of another person through any information system with intent to harm or defraud. Applicable to WhatsApp impersonation fraud. Penalty: up to 3 years imprisonment and/or fine up to PKR 5 million.

- **Section 15 — Unauthorized Issuance of SIM Cards:** Targets illegal SIM registration — a foundational enabler of WhatsApp hijacking via SIM swap. Penalty: up to 3 years imprisonment.
- **Section 16 — Cyberterrorism:** Applicable where online fraud targets critical information infrastructure. Penalty: up to 14 years imprisonment.
- **Section 18 — Electronic Fraud:** Directly criminalizes fraudulent use of information systems to obtain property or financial benefit dishonestly. Penalty: up to 2 years imprisonment and/or fine up to PKR 10 million.
- **Section 19 — Cyberstalking:** Applicable where fraud is accompanied by harassment of victims or their families.
- **Section 20 — Unauthorized Access:** Criminalizes unauthorized access to information systems — applicable to WhatsApp account takeover. Penalty: up to 3 months imprisonment or fine up to PKR 50,000.

Importantly, PECA 2016 also provides for preservation orders (Section 30), production orders (Section 31), and search and seizure powers (Section 32), which are critical tools in cybercrime investigations. However, critics have noted that Section 20's penalty is disproportionately lenient relative to the gravity of the harm caused (Cheema, 2019).

3.2 Pakistan Penal Code 1860 (PPC)

Traditional penal provisions supplement PECA 2016 in prosecuting online fraud. Section 420 PPC (cheating and dishonestly inducing delivery of property) and Section 406 PPC (criminal breach of trust) are routinely invoked in conjunction with PECA charges in cases involving mobile wallet fraud. The applicability of these provisions to digital transactions was confirmed in FIA v. Muhammad Asif (Lahore High Court, 2019), where the court held that digital financial deception falls squarely within the ambit of Section 420 PPC (Ali & Hasan, 2021).

3.3 Electronic Transactions Ordinance 2002 (ETO 2002)

The ETO 2002 provides the foundational legal recognition of electronic documents and digital signatures in Pakistan. While not a cybercrime statute per se, it establishes the legal validity of digital evidence — a critical procedural prerequisite for the prosecution of online fraud cases.

Section 36 ETO empowers courts to receive electronic records as evidence subject to authentication requirements (Government of Pakistan, 2002).

3.4 The Payment Systems and Electronic Fund Transfers Act 2007

This statute governs the regulatory framework for electronic payment systems and fund transfers in Pakistan. It confers authority on the State Bank of Pakistan to regulate payment service providers including mobile wallet operators. Section 10 mandates "reasonable measures" to prevent unauthorized fund transfers — a provision whose enforcement in the context of Easypaisa fraud has been widely criticized as inadequate (SBP, 2022).

3.5 Role of the FIA Cybercrime Wing

The FIA Cybercrime Wing, established under PECA 2016, serves as Pakistan's primary cybercrime enforcement agency. Operating from 25 provincial and regional offices, it received **over 97,000 cybercrime complaints** in 2022 alone (FIA, 2023). Despite institutional growth, the Wing faces severe challenges: a chronic shortage of trained digital forensic investigators, inadequate technological infrastructure, jurisdictional ambiguity in transnational cases, and low prosecution rates estimated at less than 10% of registered cases (Cheema, 2019).

3.6 Data Protection Lacunae

A notable gap in Pakistan's cyber law framework is the absence of a comprehensive data protection law. The Personal Data Protection Bill (PDPB), drafted in 2021 and revised in 2023, had not been enacted as of the time of writing. This legislative vacuum means that data breaches facilitating online fraud — such as unauthorized access to telecom subscriber databases or NADRA records — are inadequately addressed, and victims have no statutory right to notification or compensation for breach of their personal data (Ali & Hasan, 2021).

4. Comparative International Legal Frameworks

4.1 The Budapest Convention on Cybercrime (2001)

The Budapest Convention, adopted by the Council of Europe in 2001 and open for global accession, is the foremost international treaty on cybercrime. It harmonizes national laws, facilitates cross-border investigation and extradition, and establishes mandatory offences including illegal

access (Article 2), computer-related fraud (Article 8), and identity-related offences. Pakistan has not acceded to the Budapest Convention, a significant impediment to international cybercrime cooperation (Council of Europe, 2001). The Convention's *24/7 network* for emergency cybercrime cooperation — to which Pakistan is not connected — is routinely used by member states to preserve digital evidence across borders before it can be deleted (Gercke, 2012).

By contrast, countries such as Nigeria, Philippines, and Morocco — all facing similar cybercrime profiles to Pakistan — have acceded to or aligned their domestic laws with the Budapest Convention, enabling more effective prosecution of transnational fraud (Council of Europe, 2023).

4.2 United Kingdom: Computer Misuse Act 1990 and Fraud Act 2006

The United Kingdom's legal framework for cybercrime fraud rests on two principal statutes. The Computer Misuse Act 1990 (CMA) criminalizes unauthorized access to computer material (Section 1), unauthorized access with intent to commit further offences (Section 2), and unauthorized acts causing or risking serious damage (Section 3A). The CMA has been regularly updated — most recently by the Serious Crime Act 2015 — to address new attack vectors including credential theft tools used in WhatsApp hacking (Her Majesty's Government, 2015).

The Fraud Act 2006 provides a unified, technologically neutral fraud offence encompassing fraud by false representation, fraud by failing to disclose information, and fraud by abuse of position — all directly applicable to digital financial deception (Her Majesty's Government, 2006). The UK's Action Fraud reporting centre, operated by the City of London Police, provides a centralized national fraud reporting mechanism conspicuously absent in Pakistan's fragmented complaint architecture.

The UK further benefits from the National Cyber Security Centre (NCSC), which provides threat intelligence, active defence capabilities, and public awareness campaigns — a model that Pakistan's newly established National Cyber Emergency Response Team (NCERT) seeks to emulate but has not yet matched in capacity (Hussain & Khan, 2022).

4.3 India: Information Technology Act 2000 (Amended 2008)

India's Information Technology Act 2000, significantly strengthened by the 2008 Amendment Act, provides a comprehensive cybercrime framework with direct parallels to Pakistan's PECA 2016. Section 66C criminalizes identity theft using electronic signature or other unique identification feature; Section 66D penalizes cheating by personation using a computer resource —

directly applicable to WhatsApp impersonation fraud. Penalty: up to 3 years imprisonment and/or fine up to INR 1 lakh (Government of India, 2008).

India has further operationalized its cybercrime framework through the Indian Cyber Crime Coordination Centre (I4C) and the National Cybercrime Reporting Portal (cybercrime.gov.in), which provides a user-friendly, multilingual interface for lodging complaints and tracking case progress — a significant advance over Pakistan's comparatively inaccessible reporting mechanisms (Ministry of Home Affairs, India, 2022). India's Digital Personal Data Protection Act 2023 additionally mandates strict data fiduciary obligations, creating accountability for telecom operators whose data breaches enable SIM swap fraud.

4.4 European Union: GDPR and NIS2 Directive

The European Union's General Data Protection Regulation (GDPR), operative since May 2018, imposes strict obligations on data processors and controllers, mandating 72-hour breach notification to supervisory authorities and requiring adequate technical and organizational measures to protect personal data. In the context of online fraud, GDPR provides a regulatory backstop by holding telecom operators and financial institutions accountable for data breaches that facilitate fraud — an accountability mechanism entirely absent in Pakistan's current framework (European Parliament & Council of the European Union, 2016).

The NIS2 Directive (2022/2555/EU), replacing the original Network and Information Security Directive, further mandates cybersecurity risk management and incident reporting obligations for essential service providers including banks and telecom companies — entities whose security failures directly enable the forms of mobile wallet fraud prevalent in Pakistan (European Parliament & Council of the European Union, 2022).

4.5 Comparative Summary

The comparative analysis reveals four dimensions along which Pakistan's framework diverges significantly from international best practice: (i) the absence of a comprehensive data protection law; (ii) non-accession to the Budapest Convention and resulting limitations in international cooperation; (iii) inadequate institutional capacity and centralized reporting infrastructure relative to UK and Indian models; and (iv) disproportionately lenient penalties for

unauthorized access offences under Section 20 PECA 2016 compared to equivalent provisions in UK, Indian, and EU frameworks (Gercke, 2012; Cheema, 2019).

5. Challenges in Enforcement and Implementation

Notwithstanding PECA 2016's statutory provisions, several structural and institutional challenges critically impede the effective prosecution of online fraud in Pakistan (Ali & Hasan, 2021; FIA, 2023):

- **Digital Forensic Capacity:** Pakistan's FIA Cybercrime Wing lacks sufficient forensic laboratories and trained examiners to handle the volume and technical complexity of cybercrime cases. Evidence from mobile wallets and encrypted WhatsApp communications requires specialist extraction capabilities largely absent in provincial law enforcement.
- **Judicial Capacity:** The judiciary's limited familiarity with digital evidence standards, electronic discovery procedures, and cybercrime modus operandi contributes to low conviction rates and procedural errors that undermine prosecutions.
- **Jurisdictional Complexity:** Cybercriminals frequently operate across provincial and international boundaries. Pakistan's fragmented law enforcement architecture — with cybercrime units operating at federal, provincial, and local levels without adequate coordination — creates investigative gaps exploited by sophisticated criminal networks.
- **Anonymity of Digital Infrastructure:** The use of VPNs, anonymizing networks, prepaid SIMs, and third-party mobile wallet accounts renders the tracing and attribution of online fraud to specific individuals extraordinarily difficult.
- **Victim Reluctance:** Stigma, distrust in law enforcement, and limited awareness of complaint mechanisms result in substantial underreporting of online fraud, distorting the statistical picture and depriving policymakers of accurate data (Hussain & Khan, 2022).
- **Regulatory Gaps in FinTech:** Mobile wallet operators' Know Your Customer (KYC) protocols remain insufficiently robust to prevent the registration of fraudulent accounts. Regulatory enforcement by the SBP has been criticized as reactive rather than preventative (SBP, 2022).

6. Policy Recommendations

In light of the foregoing analysis, this monograph advances the following policy recommendations:

- **Enactment of Personal Data Protection Legislation:** The promulgation of a comprehensive Personal Data Protection Act is the single most important legislative reform required. Such legislation should mandatorily incorporate telecom data breach notification obligations and establish an independent Data Protection Authority.
- **Accession to the Budapest Convention:** Pakistan should formally accede to the Budapest Convention to access its 24/7 international cooperation network and align domestic cybercrime definitions with international standards.
- **Strengthening PECA Penalties:** Section 20 PECA 2016 penalties for unauthorized access should be substantially increased to reflect the gravity of harm caused, particularly where unauthorized access precedes financial fraud.
- **Establishment of a National Fraud Reporting Portal:** Modelled on India's cybercrime.gov.in portal and the UK's Action Fraud platform, Pakistan should develop a unified, accessible online reporting mechanism integrated with the FIA Cybercrime Wing's case management system.
- **Mandatory Biometric KYC for Mobile Wallets:** The SBP should mandate real-time biometric verification for all mobile wallet registrations and high-value transactions, eliminating the vulnerability created by CNIC-based registration alone.
- **Judicial Training:** Structured cybercrime training programmes for district and sessions court judges should be institutionalized in partnership with the Federal Judicial Academy and international bodies such as the UNODC.
- **Public Awareness Campaigns:** Coordinated public education campaigns — delivered through WhatsApp, television, and community radio — are essential to reduce the social engineering vulnerability that enables the majority of online fraud (Ali & Hasan, 2021).

7. Conclusion

Online fraud — manifesting paradigmatically in WhatsApp account hijacking and subsequent mobile wallet theft — represents one of the most dynamic and damaging challenges confronting Pakistan's digital society. Pakistan's legal framework, anchored in PECA 2016, provides a meaningful but demonstrably inadequate response: the statute criminalizes the relevant conduct,

but structural deficiencies in enforcement, judicial capacity, and regulatory oversight critically undermine its deterrent and prosecutorial effectiveness.

The comparative analysis with the Budapest Convention, UK, Indian, and EU frameworks reveals that Pakistan's most critical deficits lie not in the letter of its statute but in the absence of a data protection regime, the non-accession to international cooperative frameworks, and the underdevelopment of institutional capacity. Bridging these gaps — through legislative reform, institutional investment, and international engagement — is essential if Pakistan is to mount an effective legal response to the rapidly evolving threat of cybercrime.

The cost of inaction is not merely economic. Online fraud erodes public trust in digital financial infrastructure at precisely the moment when Pakistan most needs its citizens to embrace digital financial inclusion. A robust, internationally aligned cyber law framework is therefore not merely a matter of criminal justice — it is a precondition for Pakistan's digital future (Hussain & Khan, 2022; PTA, 2023).

References

Ali, S., & Hasan, M. (2021). *Cybercrime and digital governance in Pakistan: Legal, institutional and enforcement perspectives*. Journal of Pakistan Law and Society, *8*(2), 45–78.

Cheema, A. (2019). Evaluating the Prevention of Electronic Crimes Act 2016: A critical appraisal. *Islamabad Law Review*, *3*(1), 12–39.

Council of Europe. (2001). *Convention on Cybercrime (ETS No. 185)*. Council of Europe. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Council of Europe. (2023). *T-CY: Cybercrime Convention Committee — Status of accession*. https://www.coe.int/en/web/cybercrime/parties-observer-states

European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). *Official Journal of the European Union*, L119, 1–88.

European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). *Official Journal of the European Union*, L333, 80–152.

Federal Investigation Agency. (2023). *Annual cybercrime report 2022–2023*. Government of Pakistan. https://www.fia.gov.pk/cybercrime

Gercke, M. (2012). *Understanding cybercrime: Phenomena, challenges and legal response*. International Telecommunication Union (ITU). https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Understanding%20Cybercrime%20EN.pdf

Government of India. (2008). *Information Technology (Amendment) Act 2008* (Act No. 10 of 2009). Ministry of Law and Justice, India. https://www.meity.gov.in

Government of Pakistan. (2002). *Electronic Transactions Ordinance 2002* (Ordinance LI of 2002). Ministry of Information Technology and Telecommunication.

Government of Pakistan. (2016). *Prevention of Electronic Crimes Act 2016* (Act XL of 2016). National Assembly of Pakistan. https://www.na.gov.pk/uploads/documents/1472635250_246.pdf

Her Majesty's Government. (2006). *Fraud Act 2006* (c. 35). The Stationery Office. https://www.legislation.gov.uk/ukpga/2006/35

Her Majesty's Government. (2015). *Serious Crime Act 2015* (c. 9). The Stationery Office. https://www.legislation.gov.uk/ukpga/2015/9

Hussain, Z., & Khan, R. (2022). WhatsApp fraud and mobile financial crime in Pakistan: A socio-legal study. *South Asian Journal of Legal Studies*, *5*(3), 101–128.

Ministry of Home Affairs, India. (2022). *Annual report of the Indian Cyber Crime Coordination Centre (I4C) 2021–22*. Government of India. https://cybercrime.gov.in

Pakistan Telecommunication Authority. (2023). *Annual telecom report 2022–23*. PTA. https://www.pta.gov.pk

State Bank of Pakistan. (2022). *Payment systems review: Annual report 2021–22*. SBP. https://www.sbp.org.pk/publications/PSR