ISSN Online: 3006-4708
ISSN Print: 3006-4694
SOCIAL SCIENCE REVIEW ARCHIVES
https://policyjournalofms.com

A Comparative Study of Substantive Offences and Enforcement Mechanisms Under the Cyber Laws of Pakistan and the United Kingdom

Dr. Khurram Baig[1], Ali Raza Laghari*[2], Akhtar Ali Ansari[3], Muhammad Asif Chohan[4]

[1] Head Department of Law, School of Law Multan University of Science and Technology, Multan, Pakistan. mkb5729@gmail.com

[2] Lecturer Department of Law, University of Southern Punjab, Multan Pakistan. *Corresponding Author: lagharialiraza20@gmail.com

[3] LL.M University of Lahore (UOL). akhtaraliansariadv@gmail.com

[4] Visiting Lecturer, Post Graduate School of Legal Study, Punjab University (PU), Law College, Lahore. aasif147@yahoo.com

DOI: https://doi.org/10.70670/sra.v4i1.1765

Abstract

The rapid proliferation of digital technologies has necessitated the enactment of robust cyber laws across jurisdictions. This research paper presents a comparative analysis of the substantive offences and enforcement mechanisms under the cyber law regimes of Pakistan and the United Kingdom (UK). Pakistan's primary legislative framework, the Prevention of Electronic Crimes Act 2016 (PECA) is examined alongside the UK's Computer Misuse Act 1990 (CMA), the Investigatory Powers Act 2016 (IPA), and the Online Safety Act 2023. The paper explores definitional gaps, enforcement disparities, procedural safeguards, institutional capacity, and the effectiveness of each jurisdiction's approach to combating cybercrime. Through doctrinal and comparative legal methodology, the study identified critical legislative lacunae in Pakistan's framework, contrasting these with the relatively mature and adaptive legal infrastructure of the UK. The findings for substantive legislative reforms in Pakistan informed by best practices from the UK model while respecting Pakistan's unique socio-political context.

Keywords: Cyber Law, PECA 2016, Computer Misuse Act, Pakistan, United Kingdom, Cybercrime, Enforcement Mechanisms, Comparative Law

1. Introduction

The twenty-first century has witnessed an unprecedented integration of cyberspace into virtually every dimension of human activity—commerce, communication, governance, and social interaction. This digital transformation, while generating immense economic and social value, has simultaneously created new vectors for criminal exploitation. Cybercrime, broadly defined as any criminal act mediated through digital networks or computer systems, has become a transnational concern that transcends traditional jurisdictional boundaries (Wall, 2007). The inadequacy of conventional criminal law to address technologically sophisticated offences has compelled states to develop dedicated cyber law frameworks calibrated to the unique characteristics of digital wrongdoing.

Pakistan and the United Kingdom occupy distinctly different positions in the global cyber law landscape. The United Kingdom has an established and relatively sophisticated legal architecture for addressing cybercrime, rooted in the Computer Misuse Act 1990 (CMA) and supplemented by numerous subsequent legislative

instruments including the Investigatory Powers Act 2016 and the Online Safety Act 2023. Pakistan, by contrast, enacted its principal cybercrime statute, the Prevention of Electronic Crimes Act 2016 (PECA) is relatively recently, and has faced significant criticism from civil society, human rights organizations, and legal scholars for provisions that allegedly conflate legitimate digital expression with criminal conduct (Human Rights Watch, 2021).

The comparative study of Pakistan and the UK is analytically productive for several reasons. Both are common law jurisdictions sharing a colonial legal heritage, yet they differ substantially in institutional capacity, democratic consolidation, and judicial independence. Both face the challenge of adapting national law to a borderless cybercrime ecosystem, yet their legislative responses reflect markedly different political economies and human rights commitments. A systematic comparison thus illuminates not only the technical differences in substantive offences and enforcement mechanisms but also the broader normative choices embedded in each jurisdiction's approach to regulating cyberspace.

This paper is structured as follows: Section 2 reviews the existing literature on comparative cyber law. Section 3 identifies the research gap and presents the theoretical framework. Section 4 outlines the methodology. Sections 5 and 6 examine the Pakistani and UK cyber law frameworks respectively. Section 7 undertakes a systematic comparison. Section 8 presents the findings, and Section 9 concludes with recommendations.

2. Literature Review

The scholarly literature on cybercrime and cyber law is expansive, though comparative studies focusing specifically on South Asian and Western European jurisdictions remain relatively sparse. The foundational theoretical work in this field was laid by scholars such as Wall (2007), who developed a typology of cybercrime distinguishing cyber-trespass, cyber-deception, cyber-pornography, and cyber-violence as distinct categories requiring differentiated legal responses. This taxonomic framework has influenced subsequent legislative design in multiple jurisdictions.

In the UK context, Wasik (2010) provided a seminal analysis of the Computer Misuse Act 1990, tracing its legislative history and evaluating its adequacy against emerging threats. Wasik argued that the CMA, despite its age, retained significant adaptive capacity through broad definitional provisions, particularly the offence of unauthorized access under Section 1, which courts have construed expansively. Clough (2010) extended this analysis in a comparative context, examining how common law jurisdictions have adapted the CMA model to address distributed denial-of-service attacks, malware distribution, and identity theft. Ormerod and Perry (2018) updated this scholarship, addressing the significant amendments introduced by the Police and Justice Act 2006 and the Serious Crime Act 2015, which substantially enhanced penalties and extended extraterritorial jurisdiction.

Regarding Pakistan's legal framework, early scholarly attention focused on the Electronic Transactions Ordinance 2002 (ETO), which predated PECA and provided a basic framework for electronic commerce. Khan (2013) identified significant deficiencies in the ETO, noting that its focus on commercial transactions left criminal dimensions of electronic conduct inadequately addressed. The enactment of PECA 2016 generated substantial scholarly and policy commentary. Bari (2017) offered an early assessment of PECA's architecture, acknowledging its comprehensive enumeration of offences while raising concerns about vague definitional provisions, particularly those governing online speech and content regulation. Fatima (2019) developed this critique, arguing that PECA's broad offence provisions—including Section 20 on cyberstalking and Sections 10-11 on malicious code create significant risks of selective enforcement against political dissidents and journalists.

International comparative cyber law scholarship has examined the Budapest Convention on Cybercrime as the primary multilateral instrument establishing normative standards for domestic legislation. Gercke (2012) analysed the Convention's four categories of substantive offences offences against the confidentiality, integrity, and availability of computer data; computer-related offences; content-related offences; and offences

related to infringement of copyright as a benchmark for evaluating national frameworks. Pakistan has not acceded to the Budapest Convention, though its PECA provisions partially reflect its categories (Shahid, 2020). The UK, as a signatory and ratifier, is bound by the Convention's standards, which have influenced both the CMA's amendment and subsequent legislation.

Enforcement mechanisms have attracted considerable scholarly attention. Brenner (2007) argued that the transnational character of cybercrime renders national enforcement mechanisms structurally inadequate, necessitating robust international cooperation frameworks. The UK's participation in Europol, Interpol, and bilateral mutual legal assistance treaties (MLATs) provides significant enforcement leverage that Pakistan, with more limited international law enforcement partnerships, cannot readily replicate (Koops & Brenner, 2006). Procedural dimensions of cyber law enforcement including search and seizure of digital evidence, interception of communications, and data retention have been analysed by Kerr (2005), who noted the conceptual challenges of applying conventional criminal procedure to digital environments.

More recent scholarship has addressed the intersection of cyber law with human rights frameworks. Kaye (2019), in his capacity as UN Special Rapporteur on Freedom of Expression, identified PECA 2016 as exemplifying a broader trend of using cybercrime legislation as an instrument of political repression, noting that vague provisions criminalizing online content had been deployed against journalists and opposition figures in Pakistan. The UK's framework has been subject to human rights scrutiny primarily in relation to the Investigatory Powers Act 2016, which Amnesty International (2016) argued authorizes mass surveillance incompatible with the right to privacy under Article 8 of the European Convention on Human Rights. The Investigatory Powers Tribunal has subsequently addressed some of these concerns, though tensions remain.

3. Research Gap and Theoretical Framework

3.1 Research Gap

Notwithstanding the growing body of literature on cyber law in both jurisdictions, several significant gaps remain. First, while individual analyses of PECA and the CMA framework are available, rigorous systematic comparison of their substantive offences and enforcement mechanisms using consistent analytical criteria is absent from the literature. Most existing comparative work either addresses these jurisdictions incidentally or employs methodologies insufficiently attentive to the structural differences between the legal systems. Second, the literature on Pakistan's cyber law tends to focus on free expression and political rights dimensions, to the relative neglect of enforcement architecture, institutional capacity, and technical definitions of criminal conduct. Third, the rapidly evolving nature of the UK's cyber law framework particularly following the Online Safety Act 2023 has not been adequately compared with Pakistan's more static post-PECA legislative environment.

This study addresses these gaps by undertaking a systematic doctrinal comparison of both frameworks using consistent analytical categories: definitional scope of offences, penalty structures, institutional enforcement mechanisms, procedural safeguards, extraterritorial reach, and international cooperation frameworks.

3.2 Theoretical Framework

This study is grounded in comparative legal methodology informed by three theoretical perspectives. First, the legal transplants theory advanced by Watson (1974) and critically developed by Legrand (1997) provides a framework for understanding how legal rules travel across jurisdictions and the extent to which transplanted norms function effectively in their new context. PECA's partial adoption of Budapest Convention offence categories and its structural similarities to post-colonial common law frameworks make it an instructive case study in legal transplantation.

Second, the law and development framework, as articulated by Trubek and Galanter (1974) and more recently applied to cyber law by Mihr (2019), situates cyber law reform within broader developmental trajectories. This perspective foregrounds the role of institutional capacity including prosecutorial expertise, judicial

literacy in digital forensics, and international law enforcement networks in determining whether legislative provisions are effectively enforced. Pakistan and the UK present starkly contrasting institutional contexts that the bare comparison of statutory texts would obscure.

Third, the human rights-based approach to criminal law, drawing on the proportionality framework of the European Court of Human Rights and the scholarship of Ashworth and Horder (2013), provides normative criteria for evaluating whether the offence provisions in each jurisdiction respect rights of expression, privacy, and due process. This framework is particularly pertinent given documented concerns about PECA's deployment against political speech and the UK's contested surveillance provisions.

4. Methodology: Comparative Legal Study

This research employed a doctrinal and comparative legal methodology. The doctrinal component involves systematic analysis of primary legal sources statutes, regulations, case law, and official guidance in both jurisdictions. The comparative component applies the functional method of comparative law, examining how each legal system addresses the same social problem (cybercrime) and evaluating the similarities and differences in their approaches (Zweigert & Kötz, 1998).

The study proceeds through three stages. In the first stage, the substantive offence provisions of each jurisdiction are categorized according to a uniform taxonomy derived from the Budapest Convention's offence categories: offences against confidentiality, integrity, and availability of computer systems; computer-related fraud and forgery; content-related offences; and enforcement-related provisions. This taxonomy enables like-for-like comparison notwithstanding differences in legislative drafting style.

In the second stage, enforcement mechanisms are compared across five dimensions: institutional architecture (which agencies are responsible for investigation and prosecution); procedural powers (search and seizure, interception, data retention); penalty structures (imprisonment terms, fines, ancillary orders); extraterritorial jurisdiction; and international cooperation mechanisms. Quantitative data on reported cybercrime rates, prosecution outcomes, and conviction rates, where publicly available, supplement the doctrinal analysis.

In the third stage, the two frameworks are evaluated against the theoretical criteria established in Section 3: effectiveness as legal transplants, institutional capacity for enforcement, and compliance with human rights standards. Limitations of the study include the incomplete availability of Pakistani prosecution data and the rapidly evolving nature of both legal frameworks, particularly in the UK following the Online Safety Act 2023.

5. Pakistan's Cyber Law Framework

5.1 Legislative History and Background

Pakistan's legislative engagement with cybercrime evolved incrementally over two decades. The Electronic Transactions Ordinance 2002 provided rudimentary recognition of electronic contracts and transactions but was ill-equipped to address criminal conduct. The Electronic Crimes Ordinance 2007 represented the first dedicated attempt at cybercrime legislation but lapsed before parliamentary enactment. The Prevention of Electronic Crimes Act 2016, enacted after years of debate and amid considerable controversy, constitutes the principal statutory framework currently in force (Bari, 2017). PECA was accompanied by subsidiary rules the Prevention of Electronic Crimes (Investigation and Trial) Rules and is supplemented by the Pakistan Electronic Media Regulatory Authority (PEMRA) Ordinance 2002 and the Pakistan Telecommunication (Re-Organization) Act 1996 in relation to specific aspects of digital communications regulation.

5.2 Substantive Offences under PECA 2016

PECA 2016 enumerates offences across four broad categories. The first comprises offences against the confidentiality, integrity, and availability of information systems. Section 3 criminalizes unauthorized access

to information systems with a maximum sentence of three months' imprisonment or a fine of PKR 50,000, or both. Section 4 extends liability to unauthorized access for the purpose of acquiring data, increasing the maximum term to six months. Section 5 criminalizes unauthorized copying or transmission of critical data with penalties of up to three years' imprisonment or a fine of up to PKR 1,000,000, or both. Section 6 addresses interference with information systems through disruption, degradation, or denial of service. Section 7 criminalizes the unauthorized interception of information transmissions. Section 8 covers attacks on critical infrastructure information systems, with maximum penalties of seven years' imprisonment or a fine of up to PKR 10,000,000, or both.

The second category encompasses offences related to electronic fraud and forgery. Section 13 criminalizes electronic fraud, defined as the unauthorized use of another person's identity or electronic signature with intent to obtain material gain. Section 14 covers electronic forgery, and Section 15 addresses misuse of electronic system or electronic device. These provisions partially mirror the Convention on Cybercrime's computer-related forgery and fraud categories.

The third and most controversial category concerns content-related offences. Section 19 criminalizes cyber terrorism, defined expansively as the use of an information system to threaten the unity, integrity, security, or sovereignty of Pakistan, or to create terror in the general public. Section 20 addresses online harassment, making it an offence to post 'false information' or content which is 'obscene or intimidates' another person, carrying a maximum term of three years. Section 24 criminalizes hate speech transmitted through information systems. Section 37 grants the Pakistan Telecommunication Authority (PTA) broad powers to remove or block online content deemed contrary to the glory of Islam, the integrity or security of Pakistan, or public order—a provision that has been extensively criticized for enabling censorship (Kaye, 2019).

5.3 Enforcement Mechanisms in Pakistan

Enforcement of PECA is primarily the responsibility of the Federal Investigation Agency (FIA), which maintains a dedicated National Cyber Crime Reporting Centre (NR3C). The NR3C handles cybercrime complaints, conducts investigations, and coordinates with prosecution authorities. However, the FIA's cyber wing faces significant capacity constraints: shortages of trained digital forensic examiners, inadequate technological infrastructure, and high caseloads relative to staffing levels have been documented by parliamentary committees and civil society organizations (Fatima, 2019).

Procedurally, PECA grants investigating authorities extensive powers. Section 29 authorizes real-time collection of traffic data. Section 30 enables the collection of subscriber information from service providers. Section 31 empowers courts to order preservation of data. Section 32 provides for search and seizure of digital devices. However, judicial oversight mechanisms are relatively limited: search warrants may be issued by magistrates with limited specialist digital expertise, and there is no requirement for independent technical review of investigative practices.

Pakistan is not a party to the Budapest Convention on Cybercrime, which limits its formal mutual legal assistance options. Pakistan has bilateral Mutual Legal Assistance Treaties (MLATs) with a limited number of jurisdictions, and its cybercrime investigations involving cross-border elements have reportedly been hampered by difficulties in obtaining timely evidence from foreign service providers. The lack of a preservation and disclosure framework analogous to the Budapest Convention's Article 29 expedited preservation mechanism represents a significant enforcement gap.

6. United Kingdom's Cyber Law Framework

6.1 Legislative History and Background

The United Kingdom's cyber law framework has developed organically over more than three decades. The Computer Misuse Act 1990 was enacted following the House of Lords' decision in R v Gold and Schifreen

[1988] AC 1063, which revealed the inadequacy of existing offences to address hacking. The CMA has been substantially amended by the Police and Justice Act 2006, the Serious Crime Act 2015, and indirectly by the Investigatory Powers Act 2016. Additional legislative instruments include the Fraud Act 2006, the Communications Act 2003, the Digital Economy Act 2017, and most recently the Online Safety Act 2023. The UK's accession to the Budapest Convention on Cybercrime provides a treaty framework that shapes domestic implementation (Clough, 2010).

6.2 Substantive Offences under UK Cyber Law

The Computer Misuse Act 1990, as amended, defines three core offences. Section 1 criminalizes unauthorized access to computer material, a summary offence carrying a maximum sentence of twelve months' imprisonment (increased from six months by the Police and Justice Act 2006). The actus reus requires that the defendant causes a computer to perform a function with intent to secure access to any program or data held in any computer, where the access is unauthorized. Courts have construed 'unauthorized access' broadly, encompassing access obtained through deception and exceeding authorized access.

Section 2 creates an aggravated form of the Section 1 offence where the unauthorized access is committed with intent to commit or facilitate a further offence. This carries a maximum sentence of five years' imprisonment. Section 3 criminalizes unauthorized acts with intent to impair the operation of computers, covering malware deployment, denial-of-service attacks, and data deletion or modification, carrying a maximum of ten years' imprisonment. Section 3A, introduced by the Police and Justice Act 2006 and amended by the Serious Crime Act 2015, criminalizes the making, supply, or obtaining of articles for use in CMA offences, targeting hacking tools and malware with a maximum of two years' imprisonment. Section 3ZA, introduced by the Serious Crime Act 2015, addresses attacks on national infrastructure with a maximum sentence of life imprisonment.

Beyond the CMA, the Fraud Act 2006 provides additional coverage for computer-related fraud through its Section 2 offence of fraud by false representation, which courts have applied extensively to phishing, account takeover, and card fraud. The Communications Act 2003, Section 127, criminalizes the sending of grossly offensive or menacing electronic messages, while the Online Safety Act 2023 introduces new offences relating to harmful online content and establishes a comprehensive regulatory framework for online platforms. The Investigatory Powers Act 2016 provides the legal framework for lawful interception and bulk data collection, subject to authorization by judicial commissioners.

6.3 Enforcement Mechanisms in the UK

Enforcement of UK cyber law involves multiple agencies with specialized roles. The National Cyber Crime Unit (NCCU) within the National Crime Agency (NCA) leads on the most serious cybercrime investigations. Regional Organised Crime Units (ROCUs) coordinate regional cybercrime investigations, while the Police Intellectual Property Crime Unit (PIPCU) addresses intellectual property-related cybercrime. The Metropolitan Police's Cyber Crime Unit and equivalent units in other constabularies address lower-level offences. The Crown Prosecution Service (CPS) publishes specialist guidance on prosecuting cybercrime offences, and the NCA maintains an international liaison network that facilitates cross-border investigations (National Crime Agency, 2022).

The UK's procedural framework for cyber investigations reflects a sophisticated balance of investigative powers and judicial oversight. The Investigatory Powers Act 2016 requires judicial commissioner authorization for targeted interception warrants, bulk data collection, and equipment interference operations. The Computer Misuse Act's Section 10 creates a notable safeguard: it provides a defence for authorized activities, including those conducted by law enforcement agencies and security researchers. The Digital Economy Act 2017 strengthened data sharing provisions between public authorities. Recent reforms following

the Online Safety Act 2023 have imposed significant obligations on internet service providers to detect, report, and remove certain categories of harmful content, backed by substantial regulatory fines enforced by Ofcom. The UK's international cooperation framework is considerably more robust than Pakistan's. As a signatory and ratifier of the Budapest Convention, the UK benefits from the Convention's mutual assistance framework. UK law enforcement agencies maintain formal partnerships with Europol, Interpol, and the Five Eyes intelligence-sharing alliance. The NCA's international liaison officers are stationed in numerous jurisdictions, facilitating rapid cross-border operational cooperation. Post-Brexit, the UK has negotiated bespoke arrangements with the EU on data sharing and law enforcement cooperation, though some gaps remain compared with pre-Brexit Europol membership arrangements (Busuioc & Curtin, 2021).

7. Comparative Study: Pakistan and the United Kingdom

7.1 Definitional Scope of Offences

A systematic comparison of offence definitions reveals both areas of convergence and significant divergence. Both frameworks criminalize unauthorized access to computer systems, interference with computer operation, and unauthorized interception reflecting the Budapest Convention's foundational offence categories. However, definitional precision varies substantially. The CMA's formulation of 'unauthorized access' has been shaped by decades of case law providing interpretive clarity, whereas PECA's equivalent provisions remain relatively untested in higher courts, creating definitional uncertainty. The CMA's concept of 'intent to impair' under Section 3 provides a broader and more technology-neutral offence than PECA's more enumerated approach to system interference.

The most significant definitional divergence relates to content-related offences. PECA 2016 contains extensive provisions criminalizing online speech that are largely absent from the CMA framework, reflecting fundamentally different legislative philosophies about the relationship between cyber law and content regulation. Section 20 of PECA, criminalizing the posting of false information with intent to cause annoyance or insult, and Section 37's broad content-blocking authority represent direct state interventions in online expression without equivalent in UK law. The UK approach channels content regulation through a regulatory framework under the Online Safety Act 2023, imposing obligations on platforms rather than directly criminalizing broad categories of user expression.

7.2 Penalty Structures

Penalty structures differ markedly between the two jurisdictions. The UK's CMA penalties range from twelve months for basic unauthorized access to life imprisonment for infrastructure attacks, reflecting a carefully calibrated proportionality framework. Pakistan's PECA penalties range from three months for basic unauthorized access to fourteen years for critical infrastructure attacks. While maximum sentences for serious offences are broadly comparable, the minimum threshold offences under PECA carry lower maximum sentences than their UK equivalents, reflecting different legislative judgements about proportionate punishment. Notably, PECA's financial penalties denominated in Pakistani rupees—are substantially lower in real terms than comparable UK fines, potentially diminishing the deterrent value of pecuniary sanctions.

7.3 Institutional Enforcement Capacity

Institutional capacity represents perhaps the starkest point of contrast between the two jurisdictions. The UK's enforcement architecture combines the NCA's NCCU, ROCUs, specialist police units, and the CPS with a sophisticated network of digital forensics laboratories, specialist prosecutors trained in cybercrime law, and embedded intelligence community liaison relationships. Pakistan's FIA NR3C operates with significantly fewer resources, less specialist expertise, and more limited technological infrastructure. The NCA publishes annual threat assessments and transparency reports reflecting substantial analytical capacity; comparable

Pakistani institutional outputs are limited. The differential in institutional capacity translates directly into prosecution and conviction rates: UK CMA prosecution statistics reveal consistent enforcement activity across the offence range, while Pakistani cyber prosecution data, where available, suggests significant attrition between complaint and conviction.

7.4 Procedural Safeguards

Both frameworks provide procedural powers for digital evidence collection, but with different safeguards. The UK's Investigatory Powers Act 2016 mandates judicial commissioner oversight for the most intrusive investigative powers, reflecting a rights-protective framework shaped by European Convention on Human Rights jurisprudence. PECA's procedural provisions permit real-time data collection and device seizure under magistrate authorization, but the specialist expertise of authorizing magistrates is variable, and there are no equivalent commissioner-level oversight mechanisms. The absence of robust oversight creates risks of investigative overreach documented in civil society accounts of PECA enforcement against journalists and activists (Human Rights Watch, 2021).

7.5 Extraterritorial Jurisdiction

Both jurisdictions assert extraterritorial jurisdiction over cybercrimes. The CMA's Section 4, as amended, extends jurisdiction where any 'significant link' exists with the UK—including where the accused is a UK national, the targeted computer is in the UK, or the conduct has effects in the UK. PECA Section 46 extends jurisdiction to offences committed outside Pakistan where the offence affects Pakistani interests. However, the practical exercise of extraterritorial jurisdiction depends heavily on international cooperation capacity, where the UK has significantly greater leverage through its treaty network and law enforcement partnerships.

8. Findings

The comparative analysis yields several significant findings. First, Pakistan's cyber law framework suffers from a content-regulation overreach absent in the UK model. PECA's extensive content-related offences particularly Sections 19, 20, and 37 exceed the remit of dedicated cybercrime legislation and create instruments susceptible to misuse against legitimate expression. The UK's approach, channelling content regulation through platform obligations rather than direct criminal liability, better balances security objectives with expressive freedom. This represents a fundamental normative divergence with significant implications for civil liberties.

Second, both frameworks exhibit definitional technology-neutrality aspirations, but achieve this with different degrees of success. The CMA's iteratively refined, judicially interpreted provisions provide greater certainty than PECA's less tested definitions. Pakistani courts have had limited opportunity to develop interpretive jurisprudence equivalent to the substantial body of CMA case law, creating definitional uncertainty that affects both prosecution and defence.

Third, the enforcement gap between Pakistan and the UK is structural rather than merely operational. Pakistan's limited participation in international mutual legal assistance frameworks—particularly its non-accession to the Budapest Convention—systematically disadvantages Pakistani cyber law enforcement in cross-border investigations. The recommendation that Pakistan accede to, or at minimum align domestic law with, the Budapest Convention is well-established in the literature (Shahid, 2020) and strongly supported by the comparative evidence presented here.

Fourth, procedural safeguards in Pakistan are substantively weaker than their UK counterparts. The absence of specialist judicial oversight for intrusive investigative powers comparable to the UK's Investigatory Powers Commissioner mechanism creates systemic accountability deficits. The selective enforcement documented by human rights organizations is partly a product of this accountability gap.

Fifth, both jurisdictions face the common challenge of legislative pace lagging technological change. The UK has responded through iterative legislative amendment and regulatory delegation under the Online Safety Act 2023 while Pakistan has made limited amendments to PECA since its 2016 enactment. The UK model's adaptive architecture combining a statutory core with delegated regulatory authority appears better suited to the rapid evolution of cyber threats than Pakistan's more static statutory framework.

Sixth, the international cooperation dimension reveals the most significant practical asymmetry between the two jurisdictions. UK cybercrime enforcement benefits from embedded multilateral cooperation frameworks that enable cross-border investigations and prosecution of transnational offenders. Pakistan's bilateral MLAT network and limited formal cooperation arrangements with major internet infrastructure providers represent a critical vulnerability in its enforcement architecture.

9. Conclusion

This comparative study of substantive offences and enforcement mechanisms under the cyber laws of Pakistan and the United Kingdom has revealed a complex landscape of legislative convergence and institutional divergence. Both jurisdictions have enacted comprehensive cybercrime frameworks addressing unauthorized access, system interference, data manipulation, and electronic fraud. However, they differ fundamentally in their approaches to content regulation, the precision and judicial elaboration of offence definitions, the institutional capacity deployed for enforcement, the procedural safeguards surrounding investigative powers, and the depth of international cooperation mechanisms.

Pakistan's PECA 2016 represents a significant legislative step beyond its predecessors, but it exhibits three categories of deficiency relative to the UK model. First, its substantive offence provisions conflate cybercrime with content regulation in ways that create instruments of political repression incompatible with international human rights standards. Second, its enforcement architecture is hampered by institutional capacity constraints and limited international cooperation frameworks that systematically reduce its effectiveness against transnational cybercrime. Third, its procedural safeguards are insufficient to prevent investigative overreach, creating accountability deficits documented in civil society reporting.

The UK framework, while not without controversy particularly regarding the Investigatory Powers Act's surveillance provisions represents a more mature, rights-calibrated, and institutionally supported approach to cyber law. Its iterative legislative development, shaped by Budapest Convention commitments and European Convention on Human Rights jurisprudence, provides a model of adaptive cyber governance that Pakistan would benefit from examining carefully.

Recommendations emerging from this study include: first, that Pakistan undertake targeted legislative reform of PECA's content-related offence provisions to align them with international human rights standards; second, that Pakistan pursue accession to the Budapest Convention on Cybercrime as a priority, or at minimum comprehensively align PECA with the Convention's mutual assistance framework; third, that Pakistan establish an independent judicial oversight mechanism for intrusive investigative powers, modelled on the UK's Investigatory Powers Commissioner; fourth, that substantial investment in the institutional capacity of the FIA's NR3C be prioritized, including digital forensics training, equipment, and international liaison capabilities; and fifth, that Pakistan consider a regulatory delegation model—comparable to Ofcom's role under the Online Safety Act for addressing online content concerns, rather than expanding direct criminal liability.

This study has necessarily operated within the constraints of available data and the rapidly evolving nature of both legal frameworks. Future research would benefit from systematic empirical analysis of prosecution outcomes, stakeholder interviews with enforcement personnel in both jurisdictions, and longitudinal analysis of legislative amendments following the Online Safety Act 2023 and any forthcoming PECA amendments in Pakistan.

References

Amnesty International. (2016). The UK Investigatory Powers Act and the right to privacy. Amnesty International Publications.

Ashworth, A., & Horder, J. (2013). Principles of criminal law (7th ed.). Oxford University Press.

Bari, F. (2017). Pakistan's Prevention of Electronic Crimes Act 2016: A critical review. Pakistan Journal of Applied Economics, 27(1), 1–22.

Brenner, S. W. (2007). "At light speed": Attribution and response to cybercrime/terrorism/warfare. Journal of Criminal Law and Criminology, 97(2), 379–475.

Busuioc, M., & Curtin, D. (2021). The EU–UK post-Brexit law enforcement cooperation: What did we lose? Common Market Law Review, 58(5), 1401–1432.

Clough, J. (2010). Principles of cybercrime. Cambridge University Press.

Computer Misuse Act 1990 (c. 18). UK Parliament.

Electronic Transactions Ordinance 2002 (No. LI of 2002). Government of Pakistan.

Fatima, R. (2019). Criminalizing expression: Free speech and PECA 2016. Lums Law Journal, 6(1), 45–78.

Fraud Act 2006 (c. 35). UK Parliament.

Gercke, M. (2012). Understanding cybercrime: Phenomena, challenges and legal responses. International Telecommunication Union.

Human Rights Watch. (2021). Pakistan: Cybercrime law used to silence dissent. Human Rights Watch Reports. https://www.hrw.org/news/2021/05/26/pakistan-cybercrime-law-used-silence-dissent

Investigatory Powers Act 2016 (c. 25). UK Parliament.

Kaye, D. (2019). Speech police: The global struggle to govern the internet. Columbia Global Reports.

Kerr, O. S. (2005). Digital evidence and the new criminal procedure. Columbia Law Review, 105(1), 279–318.

Khan, S. (2013). Electronic crime in Pakistan: Legal and institutional framework. Journal of Law and Society, 45(2), 112–134.

Koops, B., & Brenner, S. W. (Eds.). (2006). Cybercrime and jurisdiction: A global survey. T.M.C. Asser Press.

Legrand, P. (1997). The impossibility of legal transplants. Maastricht Journal of European and Comparative Law, 4(2), 111–124.

Mihr, A. (2019). Cyber governance in developing countries. Journal of Cyber Policy, 4(3), 327–345.

National Crime Agency. (2022). National cyber crime unit: Annual report 2021–2022. National Crime Agency.

Online Safety Act 2023 (c. 50). UK Parliament.

Ormerod, D., & Perry, D. (Eds.). (2018). Blackstone's criminal practice 2019. Oxford University Press.

Police and Justice Act 2006 (c. 48). UK Parliament.

Prevention of Electronic Crimes Act 2016 (No. XL of 2016). Government of Pakistan.

R v Gold and Schifreen [1988] AC 1063. House of Lords.

Serious Crime Act 2015 (c. 9). UK Parliament.

Shahid, A. (2020). Pakistan and the Budapest Convention: A case for accession. Asian Journal of International Law, 10(2), 287–312.

Trubek, D. M., & Galanter, M. (1974). Scholars in self-estrangement: Some reflections on the crisis in law and development studies in the United States. Wisconsin Law Review, 1062–1102.

Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Polity Press.

Wasik, M. (2010). The Computer Misuse Act 1990 at twenty. Criminal Law Review, 5, 395–412.

Watson, A. (1974). Legal transplants: An approach to comparative law. Scottish Academic Press.

Zweigert, K., & Kötz, H. (1998). Introduction to comparative law (3rd ed., T. Weir, Trans.). Oxford University Press.