THE JOURNAL OF RESEARCH REVIEW

P-ISSN: 3006-2632	E-ISSN: 3006-2640
Vol. 2. No. 02 (April-June) 2025	Page 506-520

Beyond Borders: A Functionalist Comparative Analysis of Cybercrime Legislation in Pakistan, India, UK, and USA

Nasir Majeed	Assistant Professor, School of law, University of Gujrat, Punjab Pakistan. nasir.majeed@uog.edu.pk
Rabia Ilyas	Lecturer, School of Law, University of Gujrat, Punjab Pakistan. rabia@uog.edu.pk
Tabinda Rani	Lecturer, Department of Law, Hazara University Mansehra, KP Pakistan. mylawdocuments79@gmail.com

Abstract: *The study aims to understand how the core legislative text governing cybercrimes in Pakistan, India, United Kingdom and United States, address cybercrimes, investigative, trial and appellate jurisdictions, and international and national cooperation mechanisms. adopting a functionalist comparative research methodology, study found that Pakistani and Indian law cover broad range of offences as compare to UK and US laws. In addition, fine, imprisonment and combination of both, are common punishments as prescribed in all jurisdiction; however, Indian and Pakistani laws also provide offences that are punishable with fine only. In all jurisdictions, cybercrime cases are adjudicated in conventional court system with an exception to India which also established an appellate tribunal.The possibility of public private- partnership to combat cybercrimes is lacking in Pakistan but evident in India UK and USA. However, only Pakistani law explicitly provide provisions in context of international cooperation to handle cybercrimes.*

The study concludes that Pakistani law is broader in scope but suffers from institutional weaknesses; Indian law is balanced and the laws of UK and USA are mature but decentralized. It is expected that the present study will be helpful in understanding cybercrimes and will offer insight for policy makers to improve the existing legal framework of Pakistan.

Keywords: Beyond Borders cybercrimes, Cybercrimes, Comparative Legal Framework, Harmonized Cybercrime Policy

1.Introduction

To Williams (1955), 'a crime is an act capable of being followed by criminal proceedings having a criminal outcome. On the other hand, the term cybercrime is a term which has been borrowed from the literature and its frequent use in variety of contexts has introduced it in law (Lavigne, 2008). This term has various meanings; some analysts think that cybercrimes are offences that can only be committed by using a computer, computer networks (Zhang et al, 2012) or other form of information technology (McGuire & Dowling, 2013). Some view it as an act which is punishable by state and is committed online (Navneet, 2018). In addition, the term is not confined to a specific crime rather it covers broad range of criminal activities committed online. Various researchers have categorized cybercrimes differently from different perspectives. For instance, some researcher categories cybercrimes into crimes in which computers and computers networks are used as a tool, or these are the target of criminal activities or where these instruments are the place of criminal act or these tools are used as facility to commit traditional crimes (Subramanian & Sedita, 2006). In addition, cybercrimes may be cyber

dependent and cyber enabled crimes (Gordon, & Ford, 2002). Likewise, these crimes may be committed against property, person or institution. Similarly, Navneet classified cybercrimes into crimes against persons (malware, computer sabotage) crime against property (logic bomb, Trojan horse) and crimes against organizations (mail bomb) (Navneet, 2018). Smith categorized cybercrimes as syntactic, semantic and blended (Smith, 2015). To Huff, Desilets, & Kane (2010), cybercrimes may be semantic non-semantic and their amalgamation. Cybercrimes are different from traditional crimes and their difference may be summed up in the following five points. First of all, ordinary crime is easy to handle for law enforcement agencies as compare to cybercrimes which requires technical know-how to trace or investigate the crimes. Secondly, the question of jurisdiction in ordinary crime is not as much difficult as it in the case of cybercrimes. Thirdly, the applicable law in case of ordinary crimes is the same for the perpetrator and the victim which is not the case with cybercrimes (Chowbe, 2011). Fourthly, the damage to the property in ordinary crimes is visible and easily estimated as compare to cybercrimes where sometimes there is no damage to information system like in case of copying or unauthorized access. Lastly, there are gaps in the criminal laws dealing with cybercrimes which are exploited by the perpetrators across the globe (Jain, 2005).

As compare to ordinary crimes, the commission-rate of cybercrimes is increasing tremendously day by day. The newspapers report denial of service attacks, introducing harmful software, online frauds, password theft and identify misuse but there are large number of cybercrimes which go unreported by big institutions as they do not want to give their image in the public that they are vulnerable (Hatcher, McDonnell, & Ostfeld, 1999, Cyber Crime Overview. 2008). The increasing rate of cybercrimes and its different nature from ordinary crimes have compelled the states to respond to these crimes effectively through their legislative framework. In addition, the states keep a check on their performance regarding handling cybercrimes to improve it over the years. Pakistan has also witnessed the cybercrimes and it has also developed various frameworks to handle it effectively. Pakistan has been placed in Tier-1(role modelling status) which consists of top 49 countries with respect to cyber security laws (Global Cybersecurity Index (GCI) – ITU, 2024). Likewise, India USA and UK have also been listed in the Tier-1 category. Various researchers have examined the major statutory laws of these countries separately and comparatively. Moreover, numerous researchers have compared prevention of Electronic Crimes Act, 2016 (hereinafter PECA) with the major cybercrime related laws of India, UK and USA. However, these studies have certain methodological and contextual limitations and are not based on robust comparative methodology and have failed to examine the scope of cybercrimes, jurisdictional comparison and the legal framework for national or international cooperation in these jurisdictions. A comparative analysis of Pakistani, Indian, English and American legislative text is necessary to understand how these four countries view and respond to cybercrimes. The present study intends to fill this gap since its aim is to understand these issues in these four jurisdictions. The present study examines the scope of cybercrimes, jurisdictional issues and the cooperation framework in PECA, 2016, Information Technology Act (hereinafter IT ACT), 2000, The Computer Misuse Act (hereinafter CMA), 1998 and the Computer Fraud and Abuse Act (hereinafter CFAA), 1986. In addition, other amending and by laws have also been consulted to have broader understanding of the scope of cybercrimes, jurisdictional matters and framework related to cooperation in these statutes. The present study revolves around four research question; what is the scope of cybercrimes and punishments in Pakistan, India, United Kingdom and United States of America? How jurisdiction for investigation, prosecution, and trial of cybercrimes structured in Pakistan, India, UK and USA? What legal provisions exist in these jurisdictions to promote public-private partnerships in addressing cyber threats? What are the similarities and differences in the scope of cybercrimes, jurisdiction and cooperative mechanism in these jurisdictions?

Other than introductory section, the present study has five sections. The second section critically reviews the existing literature to identify the gaps in knowledge, the third section describes the methodology, and the fourth section highlights the major acts related to cybercrimes in Pakistan, India,

UK and USA. The fifth section offers the findings of the present study and the last section concludes the study.

2.Literature Review

There are numerous studies carried out by Pakistani and foreign authors on the cyber laws in Pakistan and abroad. In the Pakistani context, numerous authors have explored different dimension of (PECA) enacted in (2016). Gull, Khan and Nazanin (2021) are of the view that PECA violates the fundamental rights, especially the privacy of the citizen and freedom of speech. Ahmed, Zafar and Gul (2025) analyzed the impact of various amendments in PECA on democratic values, press freedom and digital regulations. They pointed out that the amendments in PECA critically undermined the democratic values and freedom of press in Pakistan. On the same line of reasoning, Khan, Tehrani and Iftikhar (2019) critically examined sections 3,4, 11 and 37 of PECA and pointed out that these sections were misused by the political strata of Pakistan to snub their opponents. Similarly, Iqbal et al (2023) explored the challenges and issues related to cyber security and cyberlaws in Pakistan. Saleem et al (2025) examined the challenges which the judges face while implementing cyber security laws including PECA in Pakistan.

Iqbal et al (2025) compared PECA with Indian IT Act (2000) by focusing on the enforcement mechanism and legislative framework. They found that both India and Pakistan developed enforcement and legislative frame work for specific cyber space criminal activities. Akhtar (2023) compared Pakistani cyber laws with the cyber laws of European union. According to the study, the European Union cyber laws are better than Pakistani laws since Pakistani laws do not take into consideration freedom of expression and speech. In addition, the implementation mechanism in PECA is not satisfactory as compared to European union's laws related to cybercrimes. Likewise, Khan et al (2024) compared PECA with the cyber laws of UK and found that Pakistani law had various loopholes regarding the terminologies used, limited scope, without satisfactory safeguard for witnesses and vague punishments. Similarly, Wajahat, Tarana and Gul (2024) conducted a comparative study of the Pakistani, English and American legal framework related to cyber stalking. They examined the enforcement mechanism, scope and efficiency of legal framework related to cyber stalking. It was found that PECA, as compare to UK and USA, did not exhaustively cover cyberstalking. They suggested to adopt best international practices in Pakistan so that cyber stalking might be addressed satisfactorily. On the other hand, Shahen, Zahid and Ahmad (2024) conducted a comparative study of challenges and possibilities of prosecuting cyberstalking crimes in Australia and Pakistan. Their study focused on the definition and social and psychological impacts of cyber stalking in Pakistan and Australia. They suggested that both the countries needed to improve their existing legal framework relating to cyberstalking especially by providing support services for the victims. Bakhsh et al (2016) carried out a comparative study of cyber laws of Pakistan with Saudi Arabia and United Arab Emirates by focusing on the definitions of cybercrimes and their related punishments. They suggested Pakistan and Saudi Arabia to follow UAE model pertaining to cyber laws.

There are a large number of studies comparing the cybercrimes legislation of various countries. For instance, Eboibi (2020) compared South African, Ethiopian and Nigerian cyber laws and recommended to enhance cybercrime implementation and institutional accountability, Ibekwe, (2015) compared the legal aspects of UK cyber laws with Nigeria, Kadir (2010) compared UK and USA cyber laws with other countries like UAE, Wang (2016) compared Chinese cyber laws with USA, UK and Singapore, and Lu et al (2010) compared Chinese and American cyber laws. On the other hand, various researchers have also compared Indian, English and American cyber laws with cyber laws of other countries. For instance, Gumbi (2018) examined South Africa's ICT regulatory framework with Kenya, India, United States and United Kingdom. He pointed out that that the cyber laws of developing countries including India and South Africa lack definitional clarity, territorial jurisdiction, incompatibility with international standards and inefficient enforcement mechanism. He suggested the developing countries

to establish a robust framework for the prosecution of cybercrimes and security of cyber infrastructure. Similarly, Singh and Pandey (2025) compared the Indian and UK's cyber laws by focusing on the legal framework, enforcement mechanism, and international cooperation. Halder & Jaishankar (2011) compared Indian, UK and USA laws on cyber gender harassment and victimization; Maheshwari, Hyman and Agrawal (2011) compared the definition of cybercrimes in India and USA. Likewise, Sahoo and Chattoraj (2022) examined the Indian, English, American and Japanese legal response to child pornography in cyber security laws.

3. Methodology

Comparative legal research refers to the research which compares positive laws of more than one legal system or jurisdictions in a scientific manner to highlight the similarities and dissimilarities between them (Rheinstein, 1937, Hage, 2014). The purpose of comparative legal research is to gain knowledge about legal systems, reforming own legal system and harmonization of laws (Smits, 2006, Eberle, 2007). Three approaches; functionalist, structural and hermeneutical are noteworthy in this type of research. Functionalist approach is concerned with the functions which different laws play in a legal system (Rheinstein, 1968) and only these laws will be compared which perform the same functions in different jurisdictions (Kamba, 1974). Functionalist approach is based on the assumptions that the problems which law resolves are similar across the legal systems and in the same way (Patterson, 1996, Zweigert, Kötz & Weir, 1998). Structural approach is concerned with structuring a legal system to view from insider's and outsider's perspective (Samuel, 2014). This approach involves the structural legal analysis of norms, rights and relations between them. Hermeneutical approach aims at identifying the culture and the mind set behind various legal rules (Legrand, 1996).

This study adopts a functionalist approach aiming to highlight the similarities and the dissimilarities in context of cybercrimes legislation in Pakistan, India, UK and USA. Relevant enactments including general, special and by-laws which discharged the same functions, were collected and used as data for the analysis. The analysis was carried out by following seven step methodologies. The first step involved the development of research objective which was to understand the laws pertaining to cybercrimes in four selective jurisdictions. At the second step, specific research questions were developed. At the third step the functionalist approach was selected as most appropriate compare methodology for conduction of this study. The non-empirical data was collected at the fourth step such as (PECA 2016, IT ACT, 2000, The Computer Misuse Act, 1990, Police and Justice Act 2006, Serious Crime Act 2015 The Computer Fraud and Abuse Act, Patriotic Act, 2016). The fifth step emphasized on analysis of collected data by focusing the similarities and dissimilarities among them. last step focused on structural presentation of the findings highlighting similarities and dissimilarities in context of cybercrime legislation across Pakistan, India, UK and USA.

4. Legal Frameworks for Cybercrimes

Over the years, Pakistan has experienced numerous acts dealing with the cybercrimes directly or indirectly. For instance, the Pakistan Telecommunication (Re organization) Act, was enacted in 1996 and introduced the regulatory body i.e., the Pakistan Telecommunication Authority; thought its objective was not to handle cybercrimes exclusively, however, various acts committed in the digital realm was under its operation. Similarly, Pakistan also enacted the Electronic Transactions Ordinance (ETO) in 2002 to regulate the mechanism related to electronic communications, transactions, and records to facilitate e-commerce. The act which was exclusively meant to handle cybercrimes in Pakistan is the Prevention of Electronic Crimes Act, enacted in 2016 (hereinafter PECA) and amended in 2025. This enactment not only defines cybercrimes but also provide penalties and procedure for investigation and handling cybercrimes. In India, the IT Act, 2000, exclusively deal with cybercrimes. This act was subsequently amended by the Information Technology (Amendment) Act, 2008 and introduced significant improvements to enhance its scope. The act was further amended in 2018 to provide more security to the digital data. In addition, the Personal Data Protection Bill, 2019 also offered

a robust framework to secure the data and aligned the Indian laws with international standards like GDPR. The major legislative text dealing with cybercrimes in U.K is the CMA1990, which was enacted to secure unauthorized access to computer systems and data. However, this act has been amended on numerous occasions to expand its scope. The Police and Justice Act 2006, though not specially meant for cybercrimes, contains various provisions which deal with cybercrimes especially its section 35 to 37,40 and 41. Similarly, The Serious Crime Act, 2015 also addresses the cybercrimes in UK by enhancing the investigative and prosecuting powers of law enforcement agencies. Likewise, Fraud Act, 2006 and Data Protection Act, 2018 also covers fraudulent cybercrimes and it protects professional data by aligning it with European Union's General Data Protection Regulation (hereinafter GDPR). In USA, the CFAA,1996 (18 U.S.C. S 1030), Electronic Communication Privacy Act, 1986, USA Patriotic Act, 2001, amended through 2022 and identity Theft Enforcement and Restitution Act, 2008 are four major enactments in context with cybercrimes.

5. Comparative Analysis of Cybercrime Legislation

Diverse legal frameworks regarding cybercrime exist in different territories because nations have chosen their own specific ways to respond to digital threats. The following discussion provides an assessment of cybercrime statutes in Pakistan alongside those in the USA and the UK based on their approaches to legal definitions and jurisdictional powers and investigative steps and international collaboration functionalities.

5.1. Scope of Cybercrimes

A. Scope of Definitions

Under PECA, there around thirty acts which have been declared offences under the act and these offences may be categorized into eight categories namely unauthorized access and data interference, misuse of identity, content related offences, cyber terrorism and national security, cyber and financial terrorism, malicious software, harassment and cyber stalking and regulatory

and corporate offences. Authorized access and data interference include unauthorized access to information system or data (section 3), unauthorized copying or transmission data (section 4), unauthorized access, coping or transmission of critical infrastructure data (section 5 and 6), interference with information system or data (section 14) and failure to secure data (section 27). Misuse of identity offences include unauthorized use of identity information (section 12), tempering with communication equipment (section 13) and spoofing (section 21 and 23). Content related offences include glorification of offence and hate speech (section 7). Against dignity of offences (section 15 and 18), and defamation (section 20). Likewise, national security includes cyber terrorism (section 8). Financial and commercial cyber offences include electronic forgery (section 9) and electronic fraud (section 10). Malicious software includes sending or spreading malicious codes (section 16) and supplying, making or obtaining devices for commission of offences (section 11). Harassment includes cyber stalking (section 17) and sexual content (section 18). Lastly, regulatory and corporate offences include unauthorized issuance of SIMs (section 19), failure to provide information (section, 26), offences by corporations and service providers (section 28 and 29), breach of confidentially and privacy (section 30) and attempt or abetment of offences (section 25). On the other hand, IT act, 2000 declares 20 acts as offences under IT act 2000 which may be accommodated in five categories namely, cyber intrusion and data security, identity theft, privacy breach, harmful online content and national security compliance. The cyber intrusion categories include the offences relating to tempering with computer and computer source document (sections 65 and 66), unauthorized access to protected systems (section 70) and receiving stolen computer resources (section 66-B). the secondary category of offences namely identity theft includes fraudulent use of passwords etc. (section 66-C) and cheating by personation (section 66-D). the privacy breach includes offences relating to capturing and transmitting private images (section, 66-E), breach of confidentiality and privacy (section 72) and disclosure of information in breach of lawful contract (section 72- A).

offences relating to harmful on-line content includes publishing or transmitting obscene material (section 67, 67-A and 67-B). non-compliance national security offences relate to cyber terrorism (section 66-F), intercepting government information (section 69), blocking access to information (section 69-A), and failure to comply with official directives (section 68 and 70-B).

Likewise, there are five offences according to the CMA, 1990 in UK which include unauthorized access to computer material (section 1), unauthorized access to computer with intent to commit further offence (section 2), unauthorized access or recklessly to impair a computer or computer program (section 3), unauthorized acts causing or creating significant risk to national security (section 3-ZA) and making, supplying or obtaining tools which may be used in computer related offences (section 3-A). On the other hand, the Computer Abuse and Misuse Act in USA declares only seven acts as offences which include unauthorized access to national security information (1030 a (1)), unauthorized access to obtain information (1030 a (2)), unauthorized access to government computers (1030 a (3)), access to defraud (1030 a (4)), recklessly or intentionally damaging to protected computer (1030 a (5)), trafficking in access credentials (1030 a (6)) and computer-based extortion (1030 a (7)).

The analysis reveals that the major focus of these four jurisdictions is on unauthorized access and data interference. Moreover, all the four jurisdictions view the commission of traditional crimes committed through computers or computer network as cybercrimes. In addition, Pakistan, India and USA's legislative text include the offences related to identify misuse in the cybercrimes. In

addition, these three jurisdictions also include the introduction of malicious software in the definition of cybercrimes. Likewise, Pakistani, Indian and American laws include threats to national security in the cybercrimes. However, there is striking difference regarding the breadth of cybercrimes in these jurisdictions. The Pakistani law enlists thirty criminal activities as cybercrimes, Indian laws enlists twenty acts as cybercrimes, American law declares seven acts as cybercrimes and UK law declares only five acts as cybercrimes. This may be due to the reason that in UK and USA, there are other laws which are also applicable on cybercrimes and the criminal acts declared cybercrimes in Pakistan and India have been declared cybercrimes under other amending, and independent statutes or by laws. In addition, Pakistani and Indian law declares hate speech, defamation and sexual content as cybercrime as compare to UK and USA. It is because of the reason that hate speech, defamation and display of sexual material has been declared cybercrimes under other laws like DPA, 2018 and obscenity laws. In addition, the breadth and depth of corporate offences is also different in these jurisdictions as PECA covers offences committed by corporations, service providers and SIM issuance, IT act has limited coverage of corporate offences, and CMA and CFAA cover individual acts and not corporations. Similarly, PECA and IT act contain definitions of offences in more detail as compare to UK and USA. There is also difference between these four jurisdictions in respect of target audience; PECA and IT act are user oriented as compare to CMA and CFAA which is system oriented.

B. Scope of Punishment/ Penalties

PECA provides three types of punishment namely imprisonment (rigorous and simple), fines, and combination of both (imprisonment and fines). For instance, the imprisonment under PECA may be rigorous or non-rigorous and may range from 6 months to 14 years. For instance, section 7 provides 6-month simple imprisonment and section 10 provides simple or rigorous imprisonment up to 14 years. Similarly, there are a few offences for which the only punishment is fine ranging from Rs. 50,000 to Rs. 10 million. For instance, section 25 (4) provides only fine as punishment for spamming which may exceed fifty thousand rupees. Likewise, there are various offences for which the punishment is imprisonment and fine both. For instance, section 22 provides both fine and imprisonment as punishment for child pornography. Similarly, IT Act 2000 in India provides five types of punishments namely imprisonment, fine and both imprisonment and fine, compensation to victims and forfeiture and seizure of property. For instance, section 66-F provides life imprisonment as punishment for cyber terrorism. Section 67-A provides imprisonment up to five years and fine not exceeding ten lakhs for

publishing or transmitting sexual content. There are various offences whose punishment is fine or imprisonment and the court has the discretion to impose either monetary punishment or imprisonment. For instance, section 66-E gives discretion to judges that they may impose fine up to two lakh or imprisonment up to three years for captures, publishes or transmits the image of a private area of any person without his or her consent by violating his right of privacy.

Similarly, the CMA, 1990 in UK provides three punishments namely imprisonment, fine and both. However, the judges have the discretion to impose fine, or imprisonment or both. There is no offence under the said act which provides only imprisonment or fine only rather all the penal section in the said act provides the options to the judges to impose any punishment upon an accused. Similarly, the computer misuse and fraud act in USA provides fine, imprisonment and both fine and imprisonment. However, there is no penal clause

in the said act which provides only fine as punishment; in addition, the option to impose fine or punishment is only for the first-time offender and only imprisonment is the punishment for the repeater offenders. For instance, 1030 a (1) provides ten years imprisonment or fine or both. It also states that the punishment for subsequent conviction will be up to 20 years if the offenders commit the offence for the second time.

The analysis indicates that imprisonment, fine and combination of both (fine and imprisonment) are the common type of punishments in PECA, (2016), IT Act (2000), CMA, (1990) and CFAMA (1986). Likewise, the judicial discretion related to imposition of punishment is also same in these four jurisdictions as the judges have the discretion to impose fine or imprisonment or both. Likewise, the courts have the power to impose aggravated punishment on repeated offender in all the four statutes. However, PECA also empowers the courts to impose aggravated punishment for serious crimes like electronic fraud. On the other hand, these four statutes are different on various counts. For instance, there is difference of provision of civil remedies under these laws. IT Act and CMAFA provides civil remedies to the victims as compare to PECA and AMA which do not provide. Similarly, there are a few offences in PECA and IT act which entail only fine as punishment as compare to CMA and CFAA which do not provide only-fine penal clause. Similarly, IT acts provides five types of punishments i.e., imprisonment, fine, both imprisonment and fine, compensation and forfeiture of property as compare to PECA, CMA and CFAA which provide three types of punishments. Likewise, the length of maximum punishment or penalty is also different in these statutes. PECA provides 14 years, IT Act provides life imprisonment, CMA offers 10 years and CFAA contains 20 years as maximum imprisonment.

5.2. Jurisdiction

A. Investigation

In Pakistan, the National Cyber Crime Investigation Agency (NCCIA) established by the federal government is authorized for inquiry, investigation and prosecution of the offences specified under this Act. In addition, the cybercrime wing of the FIA has been ceased and all the assets and liabilities have been transferred to the NCCIA. In addition, only the authorized officer of the agency can investigate the offences (section 30 of PECA, 2016). Similarly, under section 30 of the act, the investigation may be carried out by one or more joint investigation teams established by federal government and comprising of the authorized officers of NCCIA and any other law enforcement agencies. The joint investigation team may seek help from any intelligence agency for the purposes of investigation. In India, police officer not below the rank of inspector is authorized to investigate the offences under Information Technology Act, 2000 (section, 78). In addition, the cybercrime unit of the central board of investigation may also investigate the high- profile cases or inter-state offences related to cybercrimes if approved by the states or under court order (section 3 and 5 of Delhi Special Police Establishment Act, 1946). In United Kingdom, the relevant law for cybercrime is the CMA but it does not expressly

confer jurisdiction to any authority. However, some other enabling statutes like crime and Courts Act, 2013 and Police and Criminal Evidence Act, 1984, confer investigating powers to National crime Agency and Metropolitan Police cyber–Crime Unit. Accordingly, the National Cyber Crime Unit is the leading body which investigates cross border cybercrimes and the cybercrime unit of metropolitan police investigates the regional cybercrimes. In addition, the Regional

Organized Crime Units which are operationalized via Home Office & NCA units also cooperate with the Metropolitan police to handle the investigation of cybercrimes. In USA, the federal bureau of investigation, the United States secret services, home land security investigation, and department of justice have the authority to investigate the cybercrimes. The FBI has been delegated the authority by the attorney general to investigate the violation of federal criminal laws including cybercrimes (28 U.S.C. S 533). Similarly, the United States secret agency may investigate the financial and access related cyber offences committed in united states (18 U.S.C. S 3056). Likewise, Homeland security Investigations can also investigate the offences related to transnational threats, immigration violations and intellectual property violations (section 402 and 441 of the Homeland Security Act of 200). Likewise, the computer crime and Intellectual property Section of the Department of Justice is also authorized to coordinate to prosecute and oversight the investigation of cybercrimes.

The ongoing comparative analysis indicate that each country has dedicated investigating team to investigate the cybercrimes at local or national level though with different name. in addition, the investigation of cybercrimes may be carried out with the collaboration of more than one investigating agency in international or high-profile cases. Likewise, the investigation of international cybercrimes, high profile cases or national security related cybercrimes are investigated by central agency instead of local agency or police. Likewise, there is a difference of clarity on investigating powers of the investigating agencies. Both PECA and IT Act expressly authorizes specific agencies or officers who may initiate investigation as compare to CMA and CFAA which do not contain such provisions. However, other statutory or by laws empower certain agencies to carry out investigation of cybercrimes. Likewise, PECA contains provision which expressly justify the combined investigation in cybercrimes as compare to IT Act, CMA and CFAA which do not contain such collaborative or joint investigation though under certain other laws such investigation may be carried out in India, UK and USA.

B. Criminal Trials and Appeals

In Pakistan, the jurisdiction to try cybercrimes are not bestowed upon special courts. However, the federal government shall appoint presiding officer with the consultation of the respective chief justices of the high courts (section 41 of PECA, 2016). The provisions of Cr.P.C.(1898) and Qanoon-e Shahadat order (1984) will be applicable upon the trials of the cases to the extent that they are not inconsistent with any provision of PECA. Similarly, the appeal against the final order of session court will lie to high court and if order is passed by magistrate, to the court of session within thirty days of the provision of certified copy of the order (section 47 of PECA). In India, the IT Act does not create a separate judicial system to try the cases rather it relies on the general judicial system created by code of criminal procedure based on the nature of offence and the length of punishment. According to section 26 of the code, the magistrates may try the offences entailing up to 3 years imprisonment and the session court entailing punishment more than three years. However, the IT act creates appellate system and the appellate juration has been bestowed upon the Cyber Appellate Tribunal established by central government which will hear appeals against the matters or places notified by the central government (section 48 of ITA, 2000). Similarly, the appeal may also file against the decision of the tribunal to high courts on any question of fact or law arising out of such order (section 62 of Information Act, 2000).

In UK, the CMA, 1990 does not create or establish judicial hierarchy to try offences related to cybercrimes. This act only provides the definitions of offences, the penalties and the classification of the type of offences whether they are summary, either-way or indictable- only. The classification of the type of offences determines the appropriate criminal court for the trial of offences under it. For instance,

an offence declared summary or either-way offences under the act is to be tried by magistrate (Magistrates' Court Act, 1980) and the indictable- only offences will be tried by crown court (section 51 of Crime and Disorder Act, 1998). Similarly, the Computer Misuse Act does not provide appellate forum and the appeals against the decisions of judicial authority is determined by the general laws related to appeals. Accordingly, the appeal against the decision of conviction by the magistrate court will lie to crown court (section 108 of Magistrates' Courts Act), on point of law to the high court (section 111), and for judicial review to the Kings Bench Division of high court (section 28 of SCA 1981). Similarly, the appeal against the decision of crown court will lie to court of appeal (section 1,4,9 of Criminal Appeal Act 1968), and the decisions of the court of appeal to the supreme court (section 33 of Criminal Appeal Act, 1968) and against the decision of the supreme court, to the high court for judicial review or certiorari (section 28 of Senior Courts Act, 1981). Similarly, in USA, the Computer Fraud and Abuse Act does not establish judicial hierarchy to try offences related to cybercrimes. The general criminal legal framework provides the judicial forums to try the offences. For instance, section 3231 of 18 U.S.C bestows jurisdiction on districts courts (federal courts) to try all the offences which violates federal criminal laws including laws dealing with cyber offences. Similarly, the Federal Rules of Criminal Procedure provide how these trials are to be conducted. For instance, rule 6 provides that trials will be grand jury indictment, rule 7 deals with information and indictment, rule 7 deals with pre-trial motions and rule 23 deals with trial by jury. The appeals against the decisions of the district courts go to the circuit courts of appeal (28 U.S.C. section 1291) and the appeal against the decisions of the court of appeal may go the supreme court under special circumstances if there is significant question of law or the interpretation of the constitution (8 U.S.C. section, 1254).

However comparative analysis shows that all the four jurisdictions do not establish a separate or specific judicial system to try the cybercrimes rather these four jurisdictions rely on their ordinary criminal justice system and courts to try cybercrimes. Likewise, the courts apply the general evidence and procedural law to try cybercrimes instead of special rules of evidence and procedure. Likewise, the four statues share another common thing; the four statutes provide appellate forums against conviction of any type though the routes are different. However, the legal structure of these statutes is different on the appointment of judicial officers, structure of appellate forum and tribunal and terminologies used. The apporting authority of juridical officer under PECA is the federal government who will consult the chief justice of the respective province; under IT act, the ordinary judicial officers under CRPC courts system will try the cases and under CMA, the trial courts are either magisterial courts or crown courts under ordinary procedural laws. Likewise, Under CFAA, the federal district and criminal courts try the cybercrimes. Likewise, the appellate forum is also different under these four statutes. According to PECA, the first appeal goes to session court, and then to high court. Under IT act, the appeal first goes to cyber appellate tribunal and then to high court. In UK and USA, the appeals take the traditional path provided by the criminal law. Likewise, only IT act provides a specific appellate tribunal as compare to other three statutes which do not provide a dedicated tribunal to hear appeal against eh decision of trial courts. Likewise, PECA and IT act uses punishment duration criminology, CMA uses offence classification terminology and CFAA used terminology used in constitution regarding assignment of crimes.

C. Civil Trials and Appeals

In Pakistan, PECA is exclusively a penal enactment which does not contain any provision enabling the victims of cybercrimes to claim compensation. However, the general civil legal framework enables the victims to claim compensation under the tort law, contract act and the constitutional provisions like right of privacy etc. On the other hand, under section 43, 43-A and 46 of IT act 2000, a victim of cybercrimes in India may claim compensation. Section 43 states that the perpetrator shall be liable to pay damages by way of compensation to affected person in case of unauthorized access to computer system, downloading, introducing virus, damaging the computer, disrupting or denying access to

computers, destroying or deleting any information in computer or stealing code words of any computer with an intention to cause damage. Likewise, section 43-A enables the victim in case of failure to protect his data. Similarly, section 46 states that the central government will appoint an adjudicating officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government for holding an inquiry in the manner prescribed by the Central Government. Likewise, sub-clause g of 18 U.S.C. section 1030 enables an affected person, in case of damage or loss within 2 years, to maintain a civil action against the violator to obtain compensatory damages, injunctive relief or other equitable relief. On the other hand, the Computer Misuse Act in UK does not contain any provision enabling the affected person to claim damages or compensation. However, a victim may claim damages or compensation under torts law (misuse of private information or negligence or breach of confidence). Similarly, section 168 of Data Protection Act 2018 also enables a victim to claim compensation in case of material or non-material damage from data breach.

PECA, CMA and CFAA share one thing common that these statutes do not contain any provision regarding the provision of civil reliefs to victims. However, the victims may claim civil remedies under ordinary civil laws. On the other hand, IT act contains a specific provision allowing civil remedy to victims of cybercrimes. Likewise, the civil disputes due to cybercrimes are adjudicated by government appointed authorities under IT act and CFAA as compare to PECA and CMA. These four statutes differ on the point of scope and mechanism of adjudication of civil claims; the central government appoints adjudicating officer under IT act; civil litigation regarding cybercrimes is to be initiated in ordinary civil courts under CMA and civil cases can be filed directly in federal courts under CFAA. Similarly, the basis of civil claims under IT act and CFAA are in cyber legislation and civil litigation is based on general civil law or related statutes under PECA and CMA.

5.3. Co-operation to Mange Cybercrimes

A. Public Private Partnership

In Pakistan, there is no provision in the PECA which authorizes or encourages public-private partnership to manage, control or combat cybercrimes. However, there are various provision in PECA and some other laws which create a link between public and private entities to work

together to combat cybercrimes. For instance, section 37 of PECA authorizes the Pakistan telecommunication authority to require any entity (both public and private) to remove or block or issue directions for removal or blocking of access to an information through any information system if it considers it necessary in the interest of the glory of Islam or the integrity, security or defense of Pakistan or any part thereof, public order, decency or morality, or in relation to contempt of court or commission of or incitement to an offence under PECA. In addition, section 39 authorizes the courts after satisfaction that they may order service provider to provide real time or record the required information. similarly, the court may order any person in control of any information or system to provide access to such data to the authorized officer. In addition, section 39 of the PECA empowers the authorized officer of FIA to have access to and inspect the operation of any information system. On the other hand, Indian IT act, 2000 contains express provision for public-private partnership to combat cybercrimes. Section 70-B of IT Act, requires the central government to establish Indian Computer Emergency Response Team that will provide and coordinate to collect, analyze and disseminate of information regarding cyber threats and incidents. In addition, the team will also coordinate for cyber response activities, issue guidelines, advisories, vulnerability notes relating to information security practices, procedures, prevention, response and reporting of cyber incidents (sub-section 4). Likewise, subsection 6 requires the public and private service providers to provide any information to the team whenever is required. Moreover, Indian Computer Emergency Response Team and Manner of Performing Functions and Duties Rules, 2013 requires the team to interact with public and private stakeholders to seek assistance for the purposes of collection, analysis and disseminate information (rule,10).

In UK, the CMA, 1990 does not contain any provision which establish a cooperation link between public and private entities to handle cybercrimes. However, there are various statutory laws and official policies which encourage public private partnership to handle cybercrimes. For instance, section 129 encourages the government to have formal consultation with industry and service providers to develop code of practice to process public information; section 132 endorses private sectors via compliance mechanism; section 146 requires the private entities to cooperate with authorities about information exchange (Data Protection ACT, 2018). Similarly, National Cyber Security Strategy which is a government policy to handle cybercrimes, include public-private partnership as core principle to handle cybercrimes or issues. Likewise, the American Cybersecurity Information Act, 2015 encourages the private sector (non-federal entity) to share cyber threats or defensive measures for the purposes of cybersecurity with federal government or any other entity (section 104). In addition, the president policy directive establishes joint cyber coordination groups to protect cyber threats to United States of America (Directive 41).

The foregoing comparative analysis indicates that all the four jurisdictions recognize the significance of public- private cooperation to handle cybercrimes though not expressly provided in the four statutes but under other laws. Another point of similarities among the four statues is that they require the private sector to share specific information with various public institutions. It is also apparent that these four statutes acknowledge the significance of public-private partnership to secure national infrastructure and data security. The four statutes differ on the point of availability of express provision about pub-private partnership. PECA offers no direct provision requiring public-private partnership; however, it provides limited mechanism regarding public-private cooperation in section 37 and 39. Likewise, there is no statutory body like CERT-IN for public- private partnership for cyber governance. On the other hand, IT act expressly provides the Indian computer Emergency team to link private sector with public sector regarding cybercrimes in various contexts. CMA and CFAA also do not contain any provision making it possible for public-private partnership regarding cyber crimes though under other laws, private sector is required to cooperate with different government agencies to handle various cybercrimes. Moreover, the nature of public-private partnership is also different; in India and USA, it is mandatory, there is compliance and consultation framework exist in UK and Pakistani mechanism is court driven.

B. International Co-operation

Section 42 of PECA gives the discretion to federal government, when requested by the foreign entities to extend cooperation to designated foreign government, foreign agencies, international organizations and agencies for the purposes of investigations or proceedings concerning offences related to information systems, electronic communication or data or for the collection of evidence in electronic form relating to an offence or obtaining expeditious preservation and disclosure of data by means of an information system or real-time collection of data associated with specified communications or interception of data under this Act. Likewise, the federal government may also provide information to any foreign government or agencies related to any information obtained from its own investigations if it considers that the disclosure of such information might assist the other government, agency or organization in initiating or carrying out investigations or proceedings concerning any offence under PECA. On the other hand, there is no specific provision in IT act 2000 which establishes cooperative link between India and other states. However, CERT established under section 70-B may cooperate with other foreign entities for the collection and analysis and investigation of cyber incidents.

Similarly, there is no provision in the CMU dealing with the cooperation with foreign governments and entities regarding cyber threats and offences. However, various treaties and other statutory laws makes it possible that UK may engage with other countries to counter cyber threats and offences. For instance, U.K is the signatory of Budapest Convention on cybercrimes, 2001 and under this convention UK may offer or seek assistance and cooperation international entities (article 25). In addition, Crime (International Cooperation) Act,2003 (sections 1,4,7) and Extradition Act, 2003, (section 70, 137,138),

UK is engaged in international cooperation to handle cybercrimes and criminals. Similarly, there is no provision in the Computer Fraud and Abuse Act, under which USA may seek or provide assistance to international or foreign entities. However, the Cloud Act, 2018 empowers the attorney general with the approval of the secretary pf state to enter into agreements with foreign governments for mutual data access (section 2523). In addition, the Homeland Security Act,2000 also makes it possible that USA may cooperate with foreign governments regarding information sharing, analysis (section 201) cyber security (section 143).

The comparative study reveals that Pakistan, India, UK and USA acknowledge the necessity of international cooperation to fight against cybercrimes through express provision in the laws specifically enacted for combating cybercrimes or other statutory laws. Likewise, all four countries are cognizant of the need of data sharing and evidence-gathering activities to counter cross border cybercrimes. IT act, CMA and CFAA share the similarity that there is no express provision requiring or extending international cooperation as compare to PECA which contains express provision for international cooperation. Likewise, the analysis also reveals numerous dissimilarities on this point. PECA contains express provision authorizing international cooperation as compare to IT act, CMA and CFAA. Likewise, there is difference regarding the adopting various international conventions on cybercrimes. UK and USA are the signatory of Budapest Convention as compare to Pakistan and India who have not signed the said convention yet. In addition, the scope of international cooperation is also different among these four countries. For instance, Pakistan may share or collaborate legally to share information related to cybercrimes with other countries. India extends cooperation through executive arrangements; UK's international cooperation depends upon the EU guidelines and USA offers broadest international cooperation including sharing the real time data and cloud-based evidence.

6. Conclusions

The study on comparative analysis of Cybercrime Legislation in Pakistan, India, UK, and USA**,**

concludes that focus of all major statues pay attention to unauthorized access, interference with data and commission of traditional crimes through digital platform. PECA and IT act is broader in scope in terms of offences as compare to CMA and CFAA which heavily rely on supplementary statutes for the definitions of cybercrimes. The types of punishment are similar to a larger extent and dissimilar to some extent in terms of civil remedies. Pakistan and India clearly define the investigative mechanism in the statutes specifically meant for cybercrimes; whereas UK and USA depend upon general legal framework for investigation purposes. Moreover, there is no separate judicial system to try cybercrimes in four jurisdictions with the only exception that Indian law also provides specialized tribunals for cybercrimes. In addition, the civil remedies for victims of cybercrimes in Pakistan and UK are found in general civil law as compare to India and USA that provide civil remedies in the statute specially meant for cybercrimes. The private cooperation to handle cybercrimes is mandatory under Indian and USA legislation as compare to Pakistan which is court driven and UK which is compliance oriented. On the other hand, international cooperation under PECA is encouraged as compare to rest of the three statutes which do not contain any provision in this respect. Over all, PECA is broader in terms of number of criminal activities declared cyber offences but it lacks in private-cooperation and civil remedies. IT act, 2000 is more balanced and CMA and CFAA rely on inter-agency coordination and supplementary laws but lacks centralized framework.

References

Akhtar, S. (2023). *Assessing the Cybercrime Legislation in Pakistan: A Comparative Study of European Union and Pakistani Cybercrime Laws*. Available at SSRN 4555751.

Ahmed, F. A., Zafar, S., & Gul, S. (2025). Analyzing PECA Amendments: Press Freedom, Democratic Values, and Digital Regulation in Pakistan. (2025). *Traditional Journal of Law and Social Sciences*, *4*(01), 41-

51. https://ojs.traditionaljournaloflaw.com/index.php/TJLSS/article/view/191

Bakhsh, M., Mahmood, A., & Awan, I. I. (2016). A comparative analysis of cybercrime and cyberlaws in Islamic Republic of Pakistan, Kingdom of Saudi Arabia, and the United Arab Emirates. *Imam Journal of Applied Sciences*, 1(1), 9–15.

Chowbe, V. S. (2011). The concept of cyber-crime: Nature & scope. *Global Journal of Enterprise Information System*, 3(1), 72–84.

Cyber Crime Overview. (2008). Retrieved from http://cybercrimeindo.blogspot.com

Computer Misuse Act(1990). https://www.legislation.gov.uk/ukpga/1990/18/contents

Computer Fraud and Abuse Act, (1986). https://www.techtarget.com/searchsecurity/definition/Computer-Fraud-and-Abuse-Act-CFAA

Crime and Court act (2013). https://www.legislation.gov.uk/ukpga/2013/22/contents

Crime and Disorder Act, 1998 https://www.legislation.gov.uk/ukpga/1998/37/contents

Criminal Appeal Act (1968). https://www.legislation.gov.uk/ukpga/1968/19/contents

Data Protection Act (2018).https://www.legislation.gov.uk/ukpga/2018/12/contents

Eberle, E. J. (2007). Comparative law. *Ann. Surv. Int'l & Comp. L.*, 13, 93.

Electronic Communication Privacy Act, (1986). https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285

Eboibi, F. E. (2020). Concerns of cyber criminality in South Africa, Ghana, Ethiopia and Nigeria: Rethinking cybercrime policy implementation and institutional accountability. *Commonwealth Law Bulletin*, 46(1), 78–109.

Fraud Act, (2006). https://www.legislation.gov.uk/ukpga/2006/35/contents

Gordon, S., & Ford, R. (2002). Cyberterrorism? *Computers & Security*, 21(7), 636–647.

Gul, I., Khan, A. S., & Naznin, S. (2016). Critical analysis of Prevention of Electronic Crimes Act 2016 in Pakistan. *Asian Social Studies and Applied Research (ASSAR)*, 2(3).

Gumbi, D. (2018). Understanding the threat of cybercrime: A comparative study of cybercrime and the ICT legislative frameworks of South Africa, Kenya, India, the United States and the United Kingdom.

Hage, J. (2014). Comparative law as method and the method of comparative law. *Maastricht European Private Law Institute Working Paper*, (2014/11).

Halder, D., & Jaishankar, K. (2011). Cyber gender harassment and secondary victimization: A comparative analysis of the United States, the UK, and India. *Victims & Offenders*, 6(4), 386–398.

Hatcher, M., McDonnell, J., & Ostfeld, S. (1999). Computer crimes. *American Criminal Law Review*, 36, 397–400.

Huff, C., Desilets, C. T., & Kane, J. (2010). National public survey on white-collar crime. Rockville: National White-Collar Crime Center.

Ibekwe, C. R. (2015). The legal aspects of cybercrime in Nigeria: An analysis with the UK provisions. https://dspace.stir.ac.uk/bitstream/1893/22786/1/Ibekwe%20PHD%20THESIS.pdf

Iqbal, M., Talpur, S. R., Manzoor, A., Abid, M. M., Shaikh, N. A., & Abbasi, S. (2023). The Prevention of Electronic Crimes Act (PECA) 2016: Understanding the challenges in Pakistan. *Siazga*

Research Journal, 2(4), 273–282.

Iqbal, N., Siddiqui, H., Jumani, A., & Khan, T. A. (2025). A comparative study of cyber law in India and Pakistan: An analysis of legislative frameworks and enforcement mechanisms. *Journal of Law, Social and Management Sciences*, 4(1), 21–26.

Jain, A. (2005). *Cyber crime: Issues and threats*.

Kadir, R. M. (2010). The scope and the nature of computer crimes statutes: A critical comparative study. *German Law Journal*, 11(6), 609–632.

Kamba, W. J. (1974). Comparative law: A theoretical framework. *International & Comparative Law Quarterly*, 23(3), 485–519.

Khan, H., Shabbir, S. S., & Qureshi, A. N. (2024). Revamping cybercrime laws in Pakistan: A comparative analysis of Pakistan and United Kingdom.

Khan, S., Tehrani, P. M., & Iftikhar, M. (2024). Impact of PECA-2016 provisions on freedom of speech: A case of Pakistan. *Journal of Management Info*, 6(2), 7–11.

Lavigne, C. (2008). *Mirrorshade women: Feminism and cyberpunk at the turn of the twenty-first century* (Doctoral dissertation). McGill University, Montreal, Canada.

Legrand, P. (1996). How to compare now. *Legal Studies*, 16(2), 232–242.

Lu, H., Liang, B., & Taylor, M. (2010). A comparative analysis of cybercrimes and governmental law enforcement in China and the United States. *Asian Journal of Criminology*, 5, 123–135.

Maheshwari, H., Hyman, H. S., & Agrawal, M. (2011). A comparison of cyber-crime definitions in India and the United States. In *Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives* (pp. 33–45). IGI Global.

McGuire, M., & Dowling, S. (2013). Cybercrime: A review of the evidence. Summary of key findings and implications. *Home Office Research Report*, 75, 1–35.

Magistrates' Court Act, 1980 https://www.legislation.gov.uk/ukpga/1980/43/contents

Navneet. (2018). Introduction of cybercrime and its types. *International Research Journal of Computer Science*, 5(8), 435–439.

Prevention of Electronic Crimes Act, enacted in (2016). https://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2Jvbp8%253D-sg-jjjjjjjjjjjj

Patterson, D. (Ed.). (1996). *A companion to philosophy of law and legal theory* (p. 209). Oxford: Blackwell.

Pakistan Telecommunication (Re organization) Act (1996). https://www.pta.gov.pk/assets/media/pta_act_consolidated_footnotes_11012022.pdf

Police and Justice Act (2006).https://www.legislation.gov.uk/ukpga/2006/48/contents

Police and Criminal Evidence Act, 1984 https://www.legislation.gov.uk/ukpga/1984/60/contents

Qanoon-e-Shahadat Order (1984). https://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2Npa5plaw%3D%3D-sg-jjjjjjjjjjjj

Rheinstein, M. (1937). Teaching comparative law. *University of Chicago Law Review*, 5, 615.

Rheinstein, M. (1968). Comparative law—Its functions, methods and usages. *Arkansas Law Review*, 22, 415.

Sahoo, R., & Chattoraj, P. (2022). Child pornography through cyberspace: A comparative analysis of laws and criminal justice responses in India, USA, UK and Japan. *International Journal of Electronic Security and Digital Forensics*, 14(5), 433–455.

Saleem, H. A. R., Bukhtiar, A., Zaheer, B., & Farooq, M. A. U. (2025). Challenges faced by the judiciary in implementing cybersecurity laws in Pakistan. *The Critical Review of Social Sciences Studies*, 3(1), 1052–1066.

Shahen, M. B., Zahid, M.,& Ahmad Z,U.(2024). The intersection of technology and law: Challenges and opportunities in prosecuting cyberstalking cases in Australia and Pakistan.*Journal of Politics and International Studies.* 10(1):213–228.

Samuel, G. (2014). *An introduction to comparative law theory and method* (Vol. 11). Bloomsbury Publishing.

Singh, N., & Pandey, M. A. Comparison of the cybercrime prevention laws in India and the United Kingdom. *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 5 (4):874-880, APIS – 3920 – 0001 & ISSN - 2583-2344. https://ijlr.iledu.in/wp-content/uploads/2025/04/V5I493.pdf

Smith, R., Cheung, A., & Lau, T. (2015). Introduction: Cybercrime risks and responses—Eastern and Western perspectives. In *Cybercrime Risks and Responses* (pp. 1–9). London: Palgrave Macmillan.

Serious Crime Act, (2015). https://www.legislation.gov.uk/ukpga/2015/9/contents

Smits, J. M. (Ed.). (2006). *Elgar encyclopedia of comparative law*. Edward Elgar Publishing.

Subramanian, R., & Sedita, S. (2006). Are cybercrime laws keeping up with the triple convergence of information, innovation and technology? *Communications of the IIMA*, 6(1), 4.

The Identity Theft Enforcement and Restitution Act, 2008. https://www.findlaw.com/consumer/online-scams/the-identity-theft-enforcement-and-restitution-act.html

The Electronic Transactions Ordinance (2002). https://www.pakistanlaw.com/eto.pdf

The Code of Criminal Procedure (1898). https://www.fmu.gov.pk/docs/laws/Code_of_criminal_procedure_1898.pdf

The Information Technology Act (2000). https://ruralindiaonline.org/bn/library/resource/information-technology-act-2000/

USA Patriotic Act, 2001. https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act

Wajahat, J., Tarana, M., & Gul, S. (2024). Cyberstalking legal frameworks in the digital age: A comparative analysis of the United Kingdom, United States of America and Pakistan. *The Lighthouse Journal of Social Sciences*, 3(2), 1–13.

Wang, Q. (2016). *A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe*. Doctoral Thesis, Erasmus University Rotterdam. https://pure.eur.nl/en/publications/a-comparative-study-of-cybercrime-in-criminal-law-china-us-englan

Williams, G. (1955). The definition of crime. *Current Legal Problems*, 8(1), 107–130. https://sci-hub.se/https:/doi.org/10.1093/clp/8.1.107

Zhang, Y., Xiao, Y., Ghaboosi, K., Zhang, J., & Deng, H. (2012). A survey of cybercrimes. *Security and Communication Networks*, 5(4), 422–437.

Zweigert, K., Kötz, H., & Weir, J. A. (1998). *Introduction to comparative law Theory*. https://heinonline.org/HOL/LandingPage?handle=hein.journals/jrnatila12&div=50&id=&page=