QUARTERLY, PEER REVIEWED
al-amir
ISSN(P): 2790-931X ISSN(E): 2790-9328
E-Mail: editor.alamir@gmail.com

Jurisdiction of Cyber Laws in the Digital Age: A Comparative Analysis of National Legislation and International Legal Frameworks

Advocate Adeela Jabbar
Lecturer of Law / Advocate, High Court, Email: Jabbaradeela@gmail.com
Advocate Huzaifa Minhas
District Bar Association Sargodha / MPhil Linguistics, Department of English Language and Linguistics, University of Sargodha. Email: huzaifaminhas03@gmail.com

Submission Date: 22 August 2026
Review Date: 28 August 2026
Acceptance Date: 07 September 2026
Publication Date: 21 September 2026

Article Link: https://alamir.com.pk/index.php/ojs/article/view/370

Abstract

Digital technologies have changed communication and trade and information transmission across the boundaries of countries. The borderless character of digital technologies, however, has also enabled transnational cybercrime, which poses intricate legal issues with regard to territorial sovereignty, criminal jurisdiction and international cooperation. Cyber offences differ from traditional crimes in that they typically engage a number of countries, with multiple perpetrators, victims, computer systems and electronic evidence involved, making it difficult to determine the jurisdiction of the state in which an offence occurs.

This article reviews the basis and principles of the jurisdiction of cybercrime criminals and the jurisdiction of various countries on offences committed outside their geographical boundaries. It comparatively examines the legal framework of Pakistan, the United States, the United Kingdom and India with a specific focus on the extraterritorial application of cyber laws of the various countries. Moreover, it introduces the concept of international legal instruments, including the Budapest Convention on Cybercrime 2001 and the UN Convention against Cybercrime 2024, for international cooperation. Using relevant judicial decisions such as Yahoo! Inc. v. LICRA and Dow Jones & Company Inc. v. Gutnick and United States v. Ivanov, the article discusses the territorial and effects-based jurisdiction in cyberspace as applied. It highlights key issues such as overlapping jurisdictions, cross-border evidence gathering, extradition issues, and safeguarding state sovereignty. It reiterates that there is a need for greater multilateral coordination and better principles, and harmonisation of national laws, in combating transnational cybercrime.

Keywords: Cybercrime, Cyber Jurisdiction, Extraterritorial Jurisdiction, Territorial Sovereignty, PECA 2016, Budapest Convention, International Cooperation, Cross-Border Cybercrime.

1. Introduction

Today, with the advent of the Internet and advanced information technologies, the face of a modern society has changed. Digital platforms are vital to communication,

financial services, education, commerce and governmental functions. While these technological advances have brought many opportunities, they have also given new ways of committing crime that are not confined within traditional geographic limits.

Cybercrime encompasses all types of illegal activity in cyberspace, including unauthorized access to computer systems, identity theft, cyber financial fraud, cyberstalking, data theft, ransomware attacks, spreading of illegal content and attacks on critical information infrastructure. Such offences often have multiple jurisdictions. For instance, a user in Pakistan could break into a financial institution in the United States using a server in a third country, and the stolen data can be sent to a fourth jurisdiction.

When the cybercrime is committed in multiple countries, there is the question of jurisdiction: Who has the jurisdiction to investigate, prosecute and punish an offender?

Traditional criminal jurisdiction is a doctrine that states can have jurisdiction over offences committed within their territory. But as it has become clear that cyberspace is borderless, the application of this principle has become increasingly complicated. The whereabouts of the victim, the offender and any computer system as well as electronic evidence can all be different.

States have therefore increasingly incorporated provisions into their cybercrime law that reach beyond their borders, providing legal protections for their citizens, property and information systems even in the event that the crime itself takes place outside their borders.

The Prevention of Electronic Crimes Act, 2016 (PECA) has been enacted by Pakistan to tackle this issue; it refers to Section 1(3) and Section 1(4) respectively.[1] Likewise, the USA has enacted legislation like the Computer Fraud and Abuse Act (CFAA), 1986, and the UK has legislation to deal with computer related offences under the Computer Misuse Act, 1990. The Indian Information Technology Act 2000 has an express extraterritorial clause, as per Section 75 of the act.[2]

While these legislative changes have happened, there remain a number of issues of difference between national laws and the lack of a universally applicable regime for enforcement that continue to cause conflicts of jurisdiction.

This article therefore explores the foundations of cyber jurisdiction, the legislative practices of four countries and evaluates the impact of certain judicial rulings on this issue, as well as the role played by international legal instruments in shaping an effective regime for tackling transnational cybercrime.

2. Knowledge about Jurisdiction in Cyberspace

2.1 Meaning of Jurisdiction

Jurisdiction is the power of a state to enact laws, its enforcement of those laws, and to resolve conflicts (or criminal matters) within the power recognized by national and international legal systems. In criminal cases, jurisdiction is the power of a particular state to investigate a crime, arrest an accused, hold a trial and punish the wrongdoer.

The territorial sovereignty is traditionally linked to criminal jurisdiction. But the traditional technique is being undermined by cybercrime, which can have repercussions in multiple countries.

2.3 How to prevent the "Cybercrime Jurisdictional Nightmare"

Unlike traditional crime, committing cybercrime doesn't always involve the attacker being physically located in the country where the damage is being done.

For example:

The offender may operate from Pakistan.

Victim can live in the United Kingdom.

The computer system targeted may be in the United States.

Relevant evidence may be stored on the server located in Germany.

The financial proceeds may be transferred through an account in another country.

Under these conditions, multiple states could have concurrent jurisdiction over the same crime.

The major challenges are:

1. Different location of criminal activity: The location of criminal activity can be hard to determine as data passes through several networks and servers.

2. Multiple jurisdictional claims: More than one jurisdiction might have a valid legal interest in pursuing an investigation for the same offence.

3. International evidence: Electronic evidence often is subject to foreign service providers and could be subject to international legal assistance.

4. Varied national legislations: Criminal acts in one nation might not be an offence in another.

5. Sovereignty concerns: An investigative action that is carried out in a foreign country without permission can infringe on its sovereignty.

Hence, there is a need for a framework of the jurisdiction on the Internet that can be able to provide a balance between the interests of the affected states and the principles of international law.

3. Principles of Criminal Jurisdiction

There are several principles that are accepted by international law as bases for criminal jurisdiction. The same is true with cybercrime. [3]

3.1 Territorial Principle

The territorial principle will give jurisdiction to a State over offences committed on its territory.

Traditionally it can be split into two categories:

A. Subjective Territorial Principle

The state may have jurisdiction if it is a necessary part of the crime committed either from there or abroad. If, for instance, a person who is residing in Pakistan launches a cyber attack against a computer network in the United States, Pakistan could exercise jurisdiction because the crime took place in its territory.

B. Objective Territorial Principle / Functional Approach

A State has jurisdiction if the offence occurs in another State but has significant consequences in that State. In a certain scenario, the hacker is based in another country and steals the banking information of the Pakistani people, which results in financial loss in Pakistan, then the jurisdiction can be claimed by Pakistan.

3.2 Nationality Principle

The nationality principle allows a state to have jurisdiction over the acts of its citizens, even when they take place outside the state's borders. For instance, if a Pakistani citizen is involved in any cybercrime during his stay in another country then Pakistan may have jurisdiction to exercise it if there is any provision in its domestic law for the same.
This principle is explicitly stated under Section 1(3) of PECA 2016 which extends Pakistani citizenship to Pakistani citizens anywhere in the world. [4]

3.3 Passive Personality Principle

The passive personality principle is a basis for the exercise of jurisdiction if an offence is committed against one of the state's nationals, regardless of where the offending party and offence is located. If a foreigner is engaged in online financial fraud targeting a Pakistani citizen, then Pakistan might have an interest because its citizen is the victim of the fraud. This is especially applicable to cybercrime offences such as identity theft, financial crimes, cyberstalking and online harassment.

3.4 Protective Principle

The protective principle allows a state to assert jurisdiction over acts that occur outside of its territory when they endanger its essential national interests, security, or governmental functions. Such an attack, for instance, on a nation's defence systems, government databases or systems of national security may merit the protection of the jurisdiction.

3.5 Effects Doctrine

The effects doctrine permits a state to assert jurisdiction over acts that occur overseas when the acts leave a substantial or legally relevant impact within a state's borders. It is important in cyberspace because the perpetrator could be physically outside the country and inflict significant harm on citizens, businesses or institutions of the country.
The principle was illustrated in Yahoo! Inc. v. LICRA and Dow Jones & Company Inc. v. Gutnick.[5]
The effects doctrine should not be interpreted to give blanket jurisdiction over all sites that can be accessed from a given country. There must be some proper relation between the conduct and the state affected to prevent unreasonable claims of jurisdiction.

4. Legal Framework of Cyber Jurisdiction in Pakistan

4.1 Prevention of Electronic Crimes Act, 2016

The Prevention of Electronic Crimes Act, 2016 (PECA) was enacted in Pakistan to oversee and eliminate electronic crimes and to give room for investigation, prosecution and adjudication. The Act covers several aspects of cybercrime such as unauthorised access to information systems, unauthorised copying and transmission of data, electronic fraud, identity related offences, cyberstalking and offences relating to illegal online content. The most significant aspect of the extraterritorial jurisdiction provisions is Section 1.

4.2 Extraterritorial Application under Section 1 of PECA

In accordance with Section 1(2) of the act, PECA applies to the entire of Pakistan.[6]
Section 1(3) makes it clear that the Act is applicable to every citizen of Pakistan, no matter where he or she is, and also to every person who is present in Pakistan.

The Act also extends to an act done outside Pakistan by any person which is committed by him in accordance with the provisions of paragraph (4) of this section:[7]

The act is an offence under PECA; and It impacts on an individual, property, information system or data that is in Pakistan. This is important as it provides an express statute for cybercrime committed outside Pakistan.

Example: Now assume that someone living in another country has illegally accessed the banking data of a Pakistani citizen and funds have been withdrawn from a bank account in Pakistan. Section 1(4) may apply, even if the offender is not physically present in Pakistan, where a crime is committed under PECA and results in a crime affecting a person, property or data in Pakistan. In the same way, a foreign person who conducts a cyberattack on a governmental information system of Pakistan could be in the jurisdiction of PECA. Therefore, Section 1(4) indicates an effects-based approach in cyber jurisdiction and Section 1(3) introduces nationality-based jurisdiction.

4.3 International Cooperation under Section 42

International cooperation is covered in the framework of Section 42 in PECA.[8] It provides for cooperation with the foreign government, foreign entities or international organizations in the investigation and prosecution of offenses involving information systems, electronic communications and data by the Federal Government under the auspices of the designated agency.

Such cooperation may include:

- Gathering of electronic evidence.
- Retention and release of information.
- Real-time collection of traffic data.
- Assistance in criminal investigations.
- Cooperation in the area of information systems and electronic communications.

This provision embraces the fact that a cybercrime can not be investigated by only domestic law enforcement.

4.4 PECA Amendment 2025

The Prevention of Electronic Crimes (Amendment) Act, 2025 (Act II of 2025) has made substantial changes to PECA, both in its institutions and regulations.[9] One of the changes in the amendment was the introduction of a new investigative structure and the previous investigation mechanism provided by the FIA was replaced with the new system under the amendment provided by the NCCIA. It also established the Social Media Protection and Regulatory Authority, and other amendments concerning the regulation and adjudication of content on social media.

The amendments are applicable to the institutional enforcement of cyber laws. The general principle of extraterritoriality contained in Section 1(4), however, still plays a pivotal role in Pakistan's stance on cyber jurisdiction. When studying the current institutional setup, it is advisable to take into account the 2025 changes as against the original setup of 2016.

4.5 Pakistani Judicial Decisions

4.5.1 Muhammad Ayoub v. Federation of Pakistan

Case Muhammad Ayoub v. Federation of Pakistan and Others (2018 PCr.L.J. 1133) is a landmark case relating to the scope of regulation of unlawful content on social media.[10] This is an important case in Pakistan with regards to the ban on unlawful and inflammatory posts on social media.

The petitioner took recourse to the Lahore High Court after finding out that there were Facebook pages spreading inflammatory and blasphemous content. He asked the relevant authorities to block the pages and in turn investigate those who have uploaded the content. The case had raised some important issues on constitution of the state, freedom of expression and the challenges in regulating the social media which is operating outside Pakistan. The Court took into account the provisions of the Constitution of Pakistan, Article 19 and 19-A, and discussed the state's duty in respect of illegal online material. The judgment also acknowledged the challenges of regulating content on foreign platforms and the need for international cooperation and diplomacy to resolve the issue.

Legal significance: The case also shows the geographical location of an online platform does not automatically preclude the regulation of the site by a state because its content has legally relevant effects within that state. The decision should be read, however, as a decision on the question of regulations of online content and the question of constitutional obligations, in the first place, and not as a final determination of the boundaries of the criminal territorial jurisdiction under Section 1(4) of PECA.

4.5.2 Mukhtar Ahmad v. Federation of Pakistan

The other highlighted case is Mukhtar Ahmad v. Federation of Pakistan (Reported as PLD 2020 Islamabad).[11] The case has been cited in debates on the constitutional basis of the cybercrime laws of Pakistan and how the state should be able to oversee illegal activities on the internet. The legal basis for the case makes it clear that crimes committed with the aid of information systems can have results that are similar to those of conventional crimes and thus benefits from an effective legal regime. It is pertinent to issues related to digital rights and constitutional protection of rights and regulation of cybercrime. Before relying on this decision as a published judicial authority, one should get the exact reported citation, case number and full judgment of Mukhtar Ahmad v. Federation of Pakistan.

5. Comparative Analysis of Cyber Jurisdiction in Other Countries

5.1 United States of America

The U.S. has established a comprehensive legal system to combat computer-related crimes and cross-border cybercrime. The main piece of legislation is the Computer Fraud and Abuse Act of 1986 (18 U.S.C. 1030).[12]

The CFAA makes illegal several things, such as:

- Unauthorized access to protected computers.
- Unauthorized access to information using computers.
- Computer-related fraud.
- Damage to computer systems that is done knowingly.

- Some types of Cyber Extortion.

The definition of a protected computer includes computer located outside the United States but used in a manner that affects interstate or foreign commerce or the communications of the United States. This sets up a substantial jurisdictional link for the United States with some of the cyber activities of foreign computer systems.

Another key legislation is the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), 2018.[13] It expanded the definition of information in the Stored Communications Act so that a service provider stores electronic information for access by an officer or employee of another service provider and the statutory conditions are met.

Relevant Case: United States v. Ivanov (175 F. Supp. 2d 367, D. Conn. 2001). Here, a Russian national is charged with hacking into the computer systems of a U.S.-based company. The defendant claimed that the American court had no jurisdiction as the allegedly hacking was done from Russia. The U.S. District Court overruled the challenge. It pointed out that the alleged conduct caused intended and actual harmful effects in the United States. Victim company and affected computer systems were in the United States, and the effects of the alleged criminal acts were in the United States.

Legal significance: The ruling highlights the significance of the effects doctrine in attempting to determine jurisdiction over transnational cyber crime. It shows that the physical presence of an offender is not a prerequisite to a state's ability to exercise jurisdiction over a state in a case in which the conduct is connected to the state in an adequate way. But, read in conjunction with the statute and reasoning of the US District Court, it does not mean that all American cybercrime laws are going to be given unlimited extraterritorial effect.

5.2 United Kingdom

The Computer Misuse Act 1990 is the main legislation in the United Kingdom for regulating computer-related offences. The law gives a criminal sanction to unauthorized access to computer materials, intentional acts that affect computer systems and any other serious computer-related crimes. A key aspect of territorial scope is relevant to transnational cybercrime.

Section 4: Territorial Scope - Section 4 establishes that certain offences under the Computer Misuse Act may be prosecuted if the offending acts or events take place outside of the domestic jurisdiction, as long as the requirements in the section as to a significant link are met.[14]

Section 5: Significant Links - Section 5 recognizes situations which can create a serious connection to the home jurisdiction. These include conditions when: The accused was in the same domestic jurisdiction at the time of the unauthorized act; An electronic computer which was the subject of the unauthorized access was situated within that jurisdiction; In respect of certain serious offences, damage or risk of damage was suffered (or caused) within the jurisdiction. The significant-link requirement ensure that the legislation will not be applied unless there is an adequate connection to the United Kingdom.

Example: The territorial application of the Computer Misuse Act could apply to a person who accesses a computer system in England but has never been physically

present in that country. The UK approach thus illustrates a structured form of extraterritorial jurisdiction, one which is based on significant domestic connections.

5.3 India

The Information Technology Act, 2000 is the primary law in India which controls cybercrime. The Act covers offences relating to unauthorised access, damage to a computer system, cheating by personation and other electronic offences and the use of an identity. Section 75 is the most pertinent provision on the matter of the extraterritorial jurisdiction.[15]

In case of an offence committed outside India, the section 75 provides for action to be taken. Section 75 states that if any person, irrespective of his nationality, without his presence in India, commits any offences or contravention under the Information Technology Act, the said act is applicable for offences or contraventions if the requirements of the section are fulfilled. The Act covers acts or conduct based on the use of a computer, computer system or computer network situated in India, as indicated in Section 75(2).

Example: Section 75 could now be the basis for applying Indian cybercrime laws in the case of a hacker who hacks into a computer network in India from another country illegally. The provision is significant in light of its scope of application as it will now extend the applicability of Indian cyber law to Indian nationals and also computer systems situated within the territory of India. India's approach is therefore primarily based on the connection between the foreign conduct and computer infrastructure located within India.

5.4 Comparative Table

Pakistan | PECA 2016, Section 1(3) and 1(4) | Nationality + Effects on persons, property, systems or data in Pakistan

USA | CFAA, 18 U.S.C. § 1030 | Protected computers and statutory links with US commerce / communication

UK | Computer Misuse Act 1990, Sections 4-5 | Significant-link test

India | IT Act 2000, Section 75 | Foreign conduct involving computer system or network located in India

6.1 Pakistan's Approach: Pakistan has a fairly wide statutory approach, in that it encompasses Pakistani nationals committing offences overseas, and overseas nationals whose actions affect persons, property or information systems within Pakistan.

6.2 United States' Approach: The U.S. concept of protected computers and the statutory nexus between cyber activity and interstate and foreign commerce is crucial.

6.3 United Kingdom's Approach: The United Kingdom has a more formal approach, where a specified offence must have a meaningful connection with the UK.

6.4 India's Approach: India explicitly extends application of Information Technology Act to conduct overseas involving computer systems in India, regardless of the nationality of the offender.

6.5 Overall Comparison: All four countries acknowledge the need for law to intervene in response to cyber offences in cases where it is beyond territorial boundaries. The approaches that they have in their statutes, however, vary in the kind and quality of the

connection they require. Pakistan also expressly includes effects on persons, property and information systems and data within its territory. India stresses on the usage of Indian computer infrastructure, while the UK has a statute of "significant link test". The protected-computer concept is applied in the United States in combination with the requirements of federal criminal law. The differences illustrate the need for more coordination between national legal systems.

7. Recent Judicial Decisions on International Cyber Jurisdiction

Judicial rulings have been a major factor in shaping the rules of jurisdiction in the cyber world in addition to domestic legislation.

7.1 Yahoo! Inc. v. LICRA (France, 2000)

This is one of the most important early cases on the extent to which the national laws extend beyond the realm of the internet. Yahoo! Inc. was an American internet company with its online auction site accessible and for sale of Nazi-related memorabilia. French organisations, including the International League Against Racism and Anti-Semitism (LICRA), protested the fact that such material was available as French law forbade the public display and sale of Nazi-type objects and propaganda. Yahoo! had its main site in the United States, but it could be accessed by French users as well. The French court ruled that it was competent and imposed regulations to block access to the banned content by French people, with the threat of a monetary fine if Yahoo! does not heed.[16]

Yahoo! then contested the validity of the French order in a lawsuit filed against a U.S. federal court. The Ninth Circuit subsequently determined the national legal requirements were conflicting, and thus the French organizations were not subject to personal jurisdiction in the United States action.

Legal significance: The case is an example of the effects based approach to jurisdiction over the Internet. It illustrates the exercise of a state's regulatory power when online activity generates legally relevant consequences in the state. By the same time, the following American cases show that one state's jurisdiction cannot be assumed to mean that another will enforce its judgment. The case is thus of special value for the problems of conflicts between national laws, freedom of expression and territorial sovereignty in cyberspace.

7.2 Dow Jones & Company Inc. v. Gutnick (2002)

The High Court of Australia handed down this landmark judgement on 10 December 2002.[17] Dow Jones, an American media company, published an allegedly defamatory article on its online publication, Barron's. The article was placed on a server in the United States, and was downloaded and read by people in the state of Victoria in Australia. The plaintiff Joseph Gutnick commenced action in Victoria to have the publication declared defamatory on the basis that it had caused injury to his reputation in Victoria. Dow Jones disputed the jurisdiction of the Australian courts, because its servers were in the United States. The High Court disagreed with this and decided that for the purpose of the defamation action it was "published" when the material was downloaded and read by and understood by readers.

Legal significance: The ruling set a precedent for Internet defamation. It proved that jurisdiction does not have to be determined by the physical location of the server on

which the publisher is physically housed. The context in which the defamatory content is disseminated and leads to reputational damage can also be relevant. In considering the issue of harmful effects on the Internet and territorial jurisdiction the judgment is persuasive authority.

7.3 United States v. Ivanov (2001)

As mentioned above, this case was against a Russian national for hacking into a computer system owned by an American company.[18] The defendant contended that the U.S. had no jurisdiction over him, since he was operating from Russia. The court did not agree, holding the alleged conduct had "substantial impacts" within the United States.

Legal significance: The case exemplifies the use of effects based reasoning in criminal cybercrime cases, and underscores the significance of victim and affected computer system location.

7.4 Pakistan's Judicial System: Muhammad Ayoub

In Muhammad Ayoub v. Federation of Pakistan and Others (2018 PCr.L.J 1133), the Pakistani authorities show that it is not easy to control content on foreign servers. It brings attention to the connection between the domestic regulatory system, the rights of the individuals to the necessity of international cooperation.

As a whole, these judicial rulings illustrate the importance of not basing jurisdiction over a computer simply on knowing where a server or an offender is located. The nature of the conduct and the consequences thereof and the connection with the forum state should also be taken into consideration.

8. International Legal Frameworks relating to Cyber Jurisdiction

Cybercrime often transgresses national borders, necessitating international collaboration in order to successfully investigate and prosecute offenses. There are two international legal instruments that are particularly relevant to this topic.

8.1 The Budapest Convention on Cybercrime (2001)

The Convention on Cybercrime (also referred to as the Budapest Convention) was adopted under the Council of Europe in 2001 and entered into force on 1 July 2004.[19] It is one of the most significant international documents that deal with cybercrime and electronic evidence. The Convention aims to harmonize national legislation on cybercrime, to create investigative processes and enhance international cooperation between the law enforcement agencies.

It has the following main goals:

1. Creating common understanding of computer related offences.
2. Granting powers to investigate cybercrime.
3. Making preservation and collection of electronic evidence easier.
4. Strengthening interstate collaboration in providing legal assistance.
5. Facilitating cooperation in criminal investigations between countries.

Article 22: Jurisdiction - According to Article 22, the offences committed must be subject to the jurisdiction of the participating state, which must set it up:[20]

Within their territory.

- On board ships flying their national flag.

- On board aircraft registered under their laws.
- In specified circumstances, by their nationals.

It also establishes jurisdiction in some cases in which a person alleged to have committed an offence is in the jurisdiction of a state, but refuses to hand over the person to the other state, only on the basis of nationality. Significantly, Article 22(5) acknowledges there may be more than one state with jurisdiction over the same offence and provides a basis for consultation to identify the most appropriate jurisdiction for prosecution.

Article 23: Article 23 provides that the participating States shall cooperate with each other as widely as possible in the investigation and proceedings regarding cybercrime and electronic evidence.[21]

Article 25: Mutual Assistance - The participating States shall provide mutual assistance in criminal investigations involving computer systems, data and electronic evidence, according to Article 25.[22]

Article 35: 24/7 Network - Participating states shall set up a network of contact points and shall make them accessible on 24 hours, 7 days a week basis, according to Article 35.[23] This mechanism allows immediate collaboration, such as technical help, preservation of data and assistance in suspect identification.

Importance of the Budapest Convention: The Convention offers an action-oriented approach to international cooperation and acknowledges that speedy cooperation between national authorities is crucial for effective investigation of cybercrime. As of yet, though, Pakistan does not appear on the list of countries that are party to the Budapest Convention. It is therefore a timely reminder that its framework does not impose itself on Pakistan as a treaty obligation rather offers useful comparative model.

8.2 The United Nations Convention against Cybercrime (2024)

The UN General Assembly adopted the United Nations Convention against Cybercrime by resolution 79/243 of 24 December 2024.[24] It is an essential step towards the international effort to combat cybercrime in a more comprehensive global approach. The UN Convention is a universal convention that is open to states of all legal systems and regions, in contrast to the Budapest Convention that was formed under Council of Europe.

The main goals are to:

- Increased cooperation among countries in the fight against cybercrime.
- Raising the standard of investigations and prosecutions in offences related to information and communications technology systems.
- Facilitating the sharing of electronic evidence relating to serious crimes.
- Developing mechanisms for mutual legal assistance.
- Facilitating capacity building and technical cooperation.

Article 22: Jurisdiction - Article 22 lays down some jurisdictional obligations, the most important of which is based on territoriality. It also provides for states to have jurisdiction in some other situations such as offences committed against their nationals,

offences committed by their nationals, and offences aimed at the state. The provision also extends to cases where the alleged offender is in the state but does not get extradited.

The significance of the UN Convention: The Convention is important because it aims to set up a more general international system of cooperation between the nations beyond the regional system. Its legal status is different, however, to its adoption. At present, the Convention has 96 signatories and three parties and has not yet come into force, according to the United Nations Treaty Collection. Article 65 stipulates that the instrument of ratification, acceptance, approval or accession must be signed by 40 parties following 90 days for entry into force.[25] The Convention, as such, is thus an important international development but it is not yet an active treaty regime.

9. Great Challenges in Cyber Jurisdiction Enforcement

Although there have been national and international laws developed, there are still issues with the enforcement of cybercrime laws.

9.1 Conflicting Jurisdictional Claims

One cybercrime can have multiple countries involved, each claiming to have jurisdiction over investigating and prosecuting the offender. For instance, if a potential cyberattack comes from Pakistan and targets an American firm operating a server in Germany, the three states could all have jurisdiction. It could lead to competing investigations, complex legal responsibilities and issues of jurisdiction as to where offenses should be prosecuted.

9.2 Collection of Electronic Evidence Across Boundaries

Electronic evidence may be kept on cloud platforms and servers that are abroad from the investigative State. Investigators need to gain access to: IP addresses, Email records, Account information on social media, Server logs, Financial transaction records, Documents and communications in the cloud. Receiving this kind of information may involve mutual legal assistance requests, and the cooperation and authorization of foreign service providers, all of which must be done with the court's permission. Time delays between evidence being collected and being submitted to the court can give an opportunity for the offender to alter or remove significant digital evidence.

9.3 Extradition Difficulties

Extradition is a formal procedure in which a state passes an accused or convicted person to another state for trial or sentencing. Extradition can be problematic in crimes involving technology for the following reasons: The alleged conduct may not be recognised as a criminal offence by the requested state; The countries may lack an extradition treaty; The offence could be deemed political, or there might be legal exceptions; Extradition may be denied to its own nationals by any state by request; Different standards of evidence and procedure may apply. The principle of dual criminality (requiring that the conduct be an offence in both jurisdictions) can present problems.

9.4 Differences in National Cybercrime Legislation

Different countries may have different definitions for cyber offences. An activity which is criminalized in one country might be considered lawful expression or not be criminalized in another. These disparities cause problems in investigations, extradition and international cooperation.

9.5 Protection of State Sovereignty

It is not the norm for a state to engage in coercive investigative activity in another state's territory without a known lawful basis or consent of that state. For instance, unauthorized access to another country's computer network can create significant sovereignty issues. As a result, cybercrime investigations should be conducted in compliance with the international law and the territoriality of other states.

9.6 Issues of Privacy and Human Rights

Access to personal communications, private information and sensitive electronic records is often needed in cybercrime investigations. Over-surveillance, unnecessary disclosure of personal information, and disproportionate restrictions on online expression can be in breach of fundamental rights. However, legislation must strike the right balance between national security, crime prevention and privacy and freedom of expression in order to be effective against cybercrime.

10. Recommendations to Strengthen Cyber Jurisdiction

Engaging coordinated legal and institutional responses to the evolving nature of transnational cybercrime. The following are some of the steps that can enhance the effectiveness of cyber jurisdiction, more specifically in Pakistan.

10.1 Strengthening International Cooperation:

Pakistan needs to enhance bilateral and multilateral cooperation with its counterparts who are often associated with investigations into cross-border crimes. This collaboration should involve the exchange of digital evidence, preservation of electronic evidence, and help identify offenders.

10.2 Improving MLAT Procedures:

Electronic evidence should be made more readily accessible and responsive to international legal assistance procedures. Special arrangement to maintain data and to act quickly on requests would minimize loss of important evidence.

10.3 Considering Accession to Budapest Convention:

In view of the accession to the Budapest Convention, Pakistan must take a look at the legal, institutional and policy implications. If access to existing international cooperation mechanisms, such as the 24/7 network, is achievable, then Accession could offer the help needed.

10.4 Implementing International Standards:

It is recommended that Pakistan persist in the review of PECA and the other procedural laws to make them in line with internationally accepted best practices in cybercrime investigation, electronic evidence and human rights protection.

10.5 Strengthening the NCCIA:

The National Cyber Crime Investigation Agency should be adequately resourced, equipped with trained staff, updated digital forensic laboratories and technical know-how. It needs to be better equipped to work with foreign investigative bodies as well.

10.6 Developing Clearer Jurisdictional Guidelines:

More clarity is required regarding the exercise of extraterritorial jurisdiction to Section 1(4) of PECA. These guidelines should define the nature and extent of the connection between foreign criminal acts and the person, property and information system or data in Pakistan.

10.7 Protecting Fundamental Rights:

The development of cyber jurisdiction should be kept in line with constitutional protections and international human rights standards. Investigative powers should be subject to judicial control, proportionality, due process and just appropriate safeguards against abuse.

10.8 Promoting International Harmonization:

States must strive to harmonize the definitions of cyber offences, their jurisdiction and methods of collecting and sharing electronic evidence. The harmonization would eliminate some of the legal disputes and increase the chances of successful prosecution.

11. Discussion

The comparative analysis makes it clear that the traditional territorial principle of criminal jurisdiction is not adequate to combat today's increasingly complex cybercrime. Under PECA, Pakistan has introduced an express provision in Section 1(4) where by domestic cybercrime law will apply to some crimes committed outside its boundaries. The protected-computer approach in the United States is provided by the CFAA and the significant-link test approach in the United Kingdom is provided by the Computer Misuse Act. Under Section 75 of Indian Information Technology Act, India has an express extraterritorial provision.

The location of the offender/servers is not always the sole basis for jurisdiction as evidenced in judicial rulings. The context of the incident, the implications of the behaviour and the connection between the crime and the forum state could also be important.

But the exercise of extraterritorial jurisdiction is not enough to ensure prosecutions. A State may have a legitimate interest in pursuing a crime but may not be able to obtain evidence, arrest the perpetrator or enforce its judgment if the evidence, the person or the person's assets are abroad. The distinction between the existence of jurisdiction and practical jurisdiction is a key concept in grasping transnational cybercrime.

The Budapest Convention and the United Nations Convention against Cybercrime have been efforts to close this enforcement gap - by working together and providing mutual legal assistance and common procedural standards. However, international cooperation must be conducted respecting the sovereignty of the states, the domestic legal framework and the fundamental rights. But the best solution is not the extension of national jurisdiction but the creation of coordinated jurisdictional principles with effective international cooperation mechanisms.

12. Conclusion

Cyberspace has created new problems for traditional concepts of criminal jurisdiction because of the rise of virtual space. The concept of cyber space has radically challenged the traditional concepts of criminal jurisdiction. Often, cyber offences span across

several States and establishing who has jurisdiction to investigate and prosecute an offence is a challenge.

By comparing the country of Pakistan, United States, United Kingdom and India, it has been found that the judicial systems in various nations have formulated different opinions and judgments in response to this issue. Section 1(3) and Section 1(4) of PECA 2016 is used in Pakistan, the protected-computer framework is used in the United States, the significant-link test under the Computer Misuse Act 1990 is used in the United Kingdom and Section 75 of the Information Technology Act is extended in India.

There is a trend to consider the effects of activities when deciding over jurisdiction in the cases of Yahoo! Inc. v. LICRA, Dow Jones & Company Inc. v. Gutnick and United States v. Ivanov. Likewise, the Pakistani government's efforts in banning content on illegal social networks reflect the difficulties of regulating digital platforms outside the country.

Internationally, the Budapest Convention on Cybercrime 2001 has laid down some crucial procedures for cybercrime harmonisation and international collaboration. The Convention on the fight against cybercrime 2024 is another step towards creating a more comprehensive international approach to fighting transnational cyber offences but has not yet been put into force.

The analysis concludes that the enactment of sweeping extraterritorial provisions is not enough and needs to be accompanied by other measures for the effective regulation of cybercrime. States should also establish effective means to obtain electronic evidence, coordinate investigations, resolve jurisdictional disputes and enable extradition. Enhancing institutional capabilities of NCCIA, promoting cooperation with other countries and creating a more precise jurisdictional framework, and exploring membership in international cybercrime treaties, are some of the key steps for Pakistan to take towards tackling these issues.

In the end, the future of cyber jurisdiction will rely on achieving the balance between national sovereignty and international cooperation. To achieve accountability in a globalized digital society, a coherent legal structure backed by a coherent jurisdictional structure, robust enforcement measures and basic rights safeguard are necessary.

Bibliography

A. National Legislation

India. Information Technology Act, 2000. Especially Section 75.

Pakistan. Prevention of Electronic Crimes Act, 2016. Act No. XL of 2016.

Pakistan. Prevention of Electronic Crimes (Amendment) Act, 2025. Act No. II of 2025.

United Kingdom. Computer Misuse Act 1990.

United States. Clarifying Lawful Overseas Use of Data (CLOUD) Act, 2018.

United States. Computer Fraud and Abuse Act, 1986. 18 U.S.C. § 1030.

United States. Stored Communications Act. 18 U.S.C. §§ 2701-2713.

B. International Legal Instruments

Council of Europe. Convention on Cybercrime. ETS No. 185. Budapest, November 23, 2001. Entered into force July 1, 2004.

United Nations. United Nations Convention against Cybercrime. G.A. Res. 79/243, December 24, 2024. Not yet in force.

C. Table of Cases

Dow Jones & Company Inc. v. Gutnick [2002] HCA 56.

Muhammad Ayoub v. Federation of Pakistan, 2018 PCr.L.J. 1133 (Lahore High Court).

Mukhtar Ahmad v. Federation of Pakistan, PLD 2020 Islamabad (full citation and judgment to be verified before printing).

United States v. Ivanov, 175 F. Supp. 2d 367 (D. Conn. 2001).

Yahoo! Inc. v. LICRA, 169 F. Supp. 2d 1181 (N.D. Cal. 2001).

D. Official and Institutional Sources

Council of Europe. Convention on Cybercrime and Its Explanatory Report.

Pakistan. Ministry of Law and Justice. Pakistan Code: Prevention of Electronic Crimes Act, 2016.

United Kingdom. http://Legislation.gov.uk. Computer Misuse Act, 1990.

United Nations. UN Treaty Collection. Status of the United Nations Convention against Cybercrime.

United States. House of Representatives. United States Code, Title 18, Section 1030.

Refrences

1. Prevention of Electronic Crimes Act, 2016 (Pakistan), §§ 1(3)-1(4).

2. Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1986); Computer Misuse Act 1990 (UK), §§ 4-5; Information Technology Act, 2000 (India), § 75.

3. Council of Europe, Convention on Cybercrime, ETS No. 185, art. 22 (Budapest, November 23, 2001).
4. Prevention of Electronic Crimes Act, 2016 (Pakistan), § 1(3).
5. Yahoo! Inc. v. LICRA, 169 F. Supp. 2d 1181 (N.D. Cal. 2001); Dow Jones & Company Inc. v. Gutnick [2002] HCA 56.
6. Prevention of Electronic Crimes Act, 2016 (Pakistan), § 1(2).
7. Prevention of Electronic Crimes Act, 2016 (Pakistan), § 1(4).
8. Prevention of Electronic Crimes Act, 2016 (Pakistan), § 42.
9. Prevention of Electronic Crimes (Amendment) Act, 2025 (Act No. II of 2025) (Pakistan).
10. Muhammad Ayoub v. Federation of Pakistan, 2018 PCr.L.J. 1133 (Lahore High Court).
11. Mukhtar Ahmad v. Federation of Pakistan, PLD 2020 Islamabad (full citation and judgment to be verified before printing).
12. Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1986).
13. Clarifying Lawful Overseas Use of Data (CLOUD) Act, 2018 (United States).
14. Computer Misuse Act 1990 (UK), §§ 4-5.
15. Information Technology Act, 2000 (India), § 75.
16. Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisémitisme (LICRA), 169 F. Supp. 2d 1181 (N.D. Cal. 2001).
17. Dow Jones & Company Inc. v. Gutnick [2002] HCA 56.
18. United States v. Ivanov, 175 F. Supp. 2d 367 (D. Conn. 2001).
19. Convention on Cybercrime, ETS No. 185, entered into force July 1, 2004 (Budapest, November 23, 2001).
20. Convention on Cybercrime, ETS No. 185, art. 22 (2001).
21. Convention on Cybercrime, ETS No. 185, art. 23 (2001).
22. Convention on Cybercrime, ETS No. 185, art. 25 (2001).
23. Convention on Cybercrime, ETS No. 185, art. 35 (2001).
24. United Nations Convention against Cybercrime, G.A. Res. 79/243 (Dec. 24, 2024).
25. United Nations Convention against Cybercrime, G.A. Res. 79/243, art. 65 (Dec. 24, 2024) (not yet in force; requires 40 ratifications).