

CROSS-BORDER DIGITAL MEDIA AND JURISDICTIONAL CHALLENGES IN INTERNATIONAL LAW: REGULATING A BORDERLESS INFORMATION ENVIRONMENT

Amna Fazail¹, Dr. Aqsa Iram Shahzadi², Muhammad Faiq Butt^{*3}

¹Lecturer, Department of Media & Communication Studies, The Women University, Multan, Pakistan

²Assistant Professor, Institute of Media and Communication Studies, Bahauddin Zakariya University Multan,
Pakistan

³Assistant Professor, Department of Law, University of Okara, Pakistan

¹amna.fazail@wum.edu.pk, ²mrsaqsaairam@bzu.edu.pk, ³faiqbutt@uo.edu.pk

DOI: <http://doi.org/10.5281/zenodo.22704791>

Keywords

Cross-Border Digital Media;
Internet Jurisdiction; International
Law; Digital Sovereignty; Platform
Liability; Extraterritorial
Regulation; Cyber Governance;
Freedom of Expression; Data
Protection; Pakistan Cyber Law;
PECA 2016; Digital Human
Rights; Conflict of Laws;
Transnational Regulation

Article History

Received: 19 January 2026

Accepted: 04 March 2026

Published: 18 March 2026

Copyright @Author

Corresponding Author: *
Muhammad Faiq Butt

Abstract

Cross-border digital media has revolutionized communication across the world as information can be disseminated in a second at no expense of lengthy distances. The change has posed huge international law challenges, especially when it comes to determining which laws and jurisdictions apply, what effect the laws will have and how to manage cross-border digital evidence and enforce regulatory measures. Conventional principles of jurisdiction based on territory & nationality are becoming less effective to provide effective solutions for decentralized & transnational networks of digital communications.

This paper investigates the jurisdictional issues arising from a digital media that spreads across borders, from an international law perspective. It examines the conceptual concept of jurisdiction in cyberspace, illustrates some of the core issues in the governance of cyberspace raised by competing claims, and contrasts US, EU, Chinese and Indian approaches to regulation. Also explored are the normative conflicts between digital sovereignty and internationally accepted human rights, notably freedom of expression and privacy.

The examination of Pakistani legal system along with the salient challenges of implementing cyber regulation in developing jurisdictions while combating foreign digital platforms reveals that cyber laws are challenging to implement in the Pakistani context. A detailed study of the legal regime in Pakistan demonstrates that the enforcement of cyber regulation law is not an easy task amidst the practical challenges facing developing jurisdictions in combating foreign digital platforms. This study adopts the necessary literature from Pakistan that relates to the issues of surveillance, cybercrime enforcement, and jurisdictional fragmentation, such as Ahsan Iqbal Hashmi and his team's work.

The paper advocates the need for an existing global legal framework that would foster legal certainty and remove the regulatory fragmentation and gaps in the international digital legal landscape. It finds that a coordinated, minimum jurisdictional standards-based approach, based on greater international cooperation and improved human rights protection is needed to tackle the emerging needs related to digital media governance.

1. Introduction

The growing usage of digital communication technologies has revolutionized the creation, dissemination and consumption of media in an international dimension. The digital media is different from traditional media, as it is typically less geographically constrained and lacks a domestic legal structure to control information-sharing, so that information can be shared almost instantly across many states. The special role of social media platforms, online news media, videos/hot sites, streamers, and user-generated content networks in the global information ecosystem displaces the traditional ideas of sovereignty, territoriality and legal jurisdiction. Thus, cross-border media regulation is one of the most complicated issues for twenty-first century international law.¹

The growth of multinational digital platforms has intensified these challenges. Companies such as Facebook, X (formerly Twitter), YouTube, TikTok, and Instagram facilitate communication among billions of users located in different jurisdictions, each subject to distinct legal, political, and cultural norms. Content that is lawful in one country may be prohibited in another, creating tensions between national regulatory objectives and the inherently global nature of digital communication. Consequently, states increasingly seek to exercise jurisdiction over online activities that originate beyond their territorial boundaries but produce effects within their territories.² This development has generated significant debate concerning the scope of state authority in cyberspace and the compatibility of unilateral regulatory measures with established principles of international law.

The concepts of traditional jurisdictions arose in a time before the majority of legal controversies were associated with a distant place. At the time, the principles of territoriality, nationality and the

protective doctrine offered fairly simple guidelines for establishing a state's right to control its own affairs within or affecting its boundaries. Digital media challenges these notions, however: media content producers and platform operators, data processors and users can all be spread across diverse jurisdictions simultaneously. Content can be posted and uploaded in one country, stored on servers in another and viewed by people in many other countries. Content can be posted and uploaded in one country, stored on servers in another and viewed by people in many other countries. In many cases, a system like this brings about competing jurisdictions and overlap in jurisdiction claimd.³

Cross-border digital media also necessitates once more discussions about digital sovereignty. There has been a growing trend to regulate digital areas within the country, with states claiming the right to control digital spaces in their country to safeguard national security, public order, cultural beliefs and individual rights. Concurrently, international human rights principles stress the importance to protect freedom of expression, access to information and privacy in online environments. China is making balancing these competing interests increasingly difficult, with states taking different regulatory measures. Some states focus on the freedom of expression and platform autonomy while others put emphasis on state control, content moderation, data localization, and digital security. These discrepancies add to legal complexities and make it difficult to create clear cross-border standards for digital media.⁴

Technological advancements like the use of artificial intelligence, algorithmic systems of content recommendation, cloud-based systems and foreign data transfers introduce further obstacles to jurisdictional clarifications within digital media. With the help of ever deeper

¹ Dan Jerker B Svantesson, *Solving the Internet Jurisdiction Puzzle* (Oxford University Press 2017).

² Jack Goldsmith, 'Who Controls the Internet? Illusions of a Borderless World' (2007) 23 Strategic Direction.

³ Cedric Ryngaert, 'International Jurisdiction Law' *Research Handbook on Extraterritoriality in International Law* (Edward Elgar Publishing 2023).

⁴ Ashkan SHOKRI, 'Sovereignty in Cyberspace from the Viewpoint of International Law' [2025] Asian Journal of International Law 1.

technological infrastructures that defy the borders, a web-based platform is often hard to track by regulators to see where the relevant conduct is happening and what legislation may apply to it. Furthermore, there are practical challenges in the enforcement of the domestic law against the foreign platform operators, such as issues of evidence and international cooperation as well as the recognition of the authority of the domestic law.⁵

International law-wise, one must ask why the rightness of principles and doctrines are still substandard in light of the increasing importance of cross border digital media. While traditional rules of jurisdiction can still be relied upon as a (basic) matrix, many authors have since suggested the need to reinterpret or adapt them to suit the digital world. Furthermore, lack of an international treaty for regulating digital media has helped to create a complex legal landscape, with varying national regulations and enforcement tools. Therefore, international cooperation needs to be improved and a digital governance approach harmonized.⁶

This is especially true in developing countries, like Pakistan, where digital media platforms are playing a key role in political debates, economic transactions, and social engagement. Problems of jurisdiction within the context of domestic cyber law enforcement against foreign technology firms, the protection of personal information, the regulation of online content and the preservation of digital rights all raise complex jurisdictional problems. Significant recent research in Pakistan on digital privacy, digital surveillance, and digital cybercrime has exposed the challenges in applying conventional legal approaches to addressing off-the-territory digital phenomena and the need for more capable and efficient regulatory mechanisms to establish a balance between privacy and

cybercrime in the context of digital activities and communications.⁷

This paper reviews the problems of jurisdiction of digital media on an international legal perspective. It examines the conceptual pillars of digital jurisdiction, examines the key legal and operational challenges in regulating cross-border digital communications, reviews some of the key cross-country models of regulation in digital communication, and reflects on the consequences of digital sovereignty and human rights principles for multi-nation states' media regulation. The study also reviews the developing framework of the regulatory environment in Pakistan and postulates directions for future progress towards a more unified international regulatory framework that can cope with the complexities of digital media in a more interconnected world today.

2. Conceptual Foundations: Cross-Border Digital Media and International Jurisdiction

To grasp the abovementioned issues of law, one needs to consider the theoretical underpinnings of both digital communication and of international jurisdiction. The use of digital technology has changed our ways of thinking about place, territory and communication in relation to the law, as it enables information to flow freely through international borders. Thus, notions of law in a geographically bounded world are being challenged by the global nature of the information technology landscape. In this part, the concept of cross-border digital media is analyzed and even the classical principles of jurisdiction in international law and their relevance to overseeing digital media are explained. Here the concept of cross-border digital media is examined as well as the traditional principles of jurisdiction in international law and their application to the oversight of digital media.

⁵ Melissa Lukings and Arash Habibi Lashkari, 'Comparative Legal Strategies' *Understanding cybersecurity law in data sovereignty and digital governance: An overview from a legal perspective* (Springer 2022).

⁶ Malcolm N Shaw, 'Does the United Nations Have a Future? If so, What May That Be?' *Reimagining the International Legal Order* (Routledge 2023).

⁷ Muhammad Faiq Butt and others, 'THE RIGHT TO PRIVACY IN THE AGE OF SURVEILLANCE: LEGAL PROTECTIONS IN PAKISTAN' (2024) 2 ASSAJ 1449.

2.1 Cross-Border Digital Media: Meaning and Characteristics

The term “cross-border digital media” describes the production, distribution, transmission and uptake of content produced within a Digital Media Art realm using internet-based communication technologies and delivered to audiences that cross national borders. It covers all of the social networking websites and all of the social video platforms as well as any online newspapers, streaming platforms, blogs, podcasts and other user-generated content. Digital media, on the other hand, works in a networked environment where geographies have a much more weak impact on the spread of information than in traditional media, which tends to be established within well-known geographical boundaries.⁸

One of the hallmarks of the digital media is its ability to transmit to the world in real time. A news story written in one country can be viewed in a second's view within thousands of miles of that country. Likewise, users will often be exposed to posts on social media, live-streamed events, and digital ads that are visible in different jurisdictions around the world. This has helped to create an "international public sphere" of information that is transmitted mostly outside of physical boundaries.⁹

They also have particular characteristics, including multiple actors across various jurisdictions. Participating content creators, users, platform operators, advertisers, data processors and hosting providers may be informed of in separate countries. Its decentralized organization makes it difficult to define which legal system would be applicable in case of problems with digital communications. This makes it difficult, if not impossible, for regulatory bodies to decide on the

right forum to do things adjudication and enforcement.¹⁰

These challenges are further exacerbated by the economic importance of trans-border digital media. The digital platforms are now big global industries that rely on cross-border data transfers, cloud computing, and provide services to a global customer base via business model that crosses national boundaries. As a result, issues of international trade, data governance, privacy and digital sovereignty become coupled with a myriad of questions of jurisdiction.

2.2 Traditional Principles of Jurisdiction in International Law

The law of jurisdiction in international law can be seen as the subject of three fundamental principles that are still valid. Jurisdiction is one of the essential elements of State sovereignty. International law: the power of a state to make, interpret and apply the law. In the traditional view, jurisdictional authority has been provided upon the basis of traditional principles that strive to avoid conflicts between jurisdictions and ensure legal certainty.¹¹

The territoriality principle is the most significant of these principles: it gives the authority to the state over people, activities and events within its territory. Territorial jurisdiction has always been the cornerstone of international legal order because it has been founded on the idea of the equality and independence of the states. By this, a rule, legal power is normally associated with a special geographic place.¹²

The second basis of jurisdiction is the nationality principle, that allows states to control the conduct of nationals where ever it occurs. This principle is based on the fact that there is an ongoing relationship between a state and its nationals, irrespective of their whereabouts. Nationality

⁸ Dan Jerker B Svantesson, *Solving the Internet Jurisdiction Puzzle* (Oxford University Press 2017).

⁹ Jack Goldsmith, 'Who Controls the Internet? Illusions of a Borderless World' (2007) 23 Strategic Direction.

¹⁰ Laura E Little, 'Internet Defamation, Freedom of Expression, and the Lessons of Private International

Law for the United States' (2012) 14 European Yearbook of Private International Law 2013.

¹¹ Jan Klabbbers, *International Law* (Cambridge University Press 2020).

¹² Cedric Ryngaert, 'International Jurisdiction Law' *Research Handbook on Extraterritoriality in International Law* (Edward Elgar Publishing 2023).

jurisdiction is a basis for determining jurisdiction found in many states in areas of taxation, criminal law, and national security.

The other generally recognized basis is the passive personality principle which justifies jurisdiction of a state over crimes perpetrated against its nationals abroad. While once problematic in many respects, this principle is now part of the international law of today, despite the controversy that rages over it generally, it has been extended in the context of transnational crimes and acts of terrorism.

Lastly, the universality doctrine allows this basis for jurisdiction over certain very serious offenses even if they happen in a more distant part of the world or are committed by different nations' nationals. Universal jurisdiction has traditionally been seen as a mechanism to stop widespread and abhorrent offenses against international law, such as piracy, genocide, war crimes and crimes against humanity, and is based upon the international community's common concern.¹³

These jurisdictional principles emerged in a system of international relations that was internationalized in a territorialized sense. These jurisdictional principles developed in an international system of principles which itself was territorialized. When conduct takes place in digital sphere, beyond geographical boundaries, its use is much more complex.

2.3 Jurisdiction in Cyberspace

The advent of cyberspace has problematized and undermined the traditional logic and rules of jurisdiction. Physical activities take place in a location while online activities are likely to have multiple jurisdictions involved at the same time. This digital content can be produced in countries elsewhere, kept in a server in other countries, used for processing through the cloud over spans of several states and from many other locations around the world. This gives rise to a lack of clarity

as to the actual location of the conduct, and which state has the more substantial jurisdictional interest.¹⁴

Finding where digital activities take place is one of key challenges. Determining the territorial nexus of the court or regulatory authority for jurisdiction is often a difficult task, and a court or regulator may dispute its required jurisdiction. Court or regulator jurisdiction is often unclear and may involve a question as to what territorial nexus is necessary to have jurisdiction. For instance, if a party publishes defamatory information on a social media channel, it could be harmful to its reputation in more than one country. Likewise, and as a second example, something that is illegal in one legal jurisdiction may be legal in another. In such a case, two or more states can both claim jurisdiction over the same activity which can lead to multiple States asserting overlapping claims.

For instance, the global nature of digital media, which persists in bolstering reliance on the doctrine of the effects and to this day allows jurisdiction to be established because of acts based on behavior that takes place outside a state's territory but has significant effects within that territory. That has become a doctrine often used by governments to shore up regulations of foreign digital platforms impacting domestic consumers. But, due to its over-dependence on the implementation of effects based jurisdiction, the concerns of excessive extraterritorial control over the state and issues of the sovereignty of other states have been raised.¹⁵

An additional problem crops up because of the contrast in between legal, or legislative competence to make laws, and non-legislative, or execution competence, to implement laws. States can argue that they have jurisdiction to regulate online behavior when online platforms concern themselves with their interests but such enforcement is difficult against foreign platform

¹³ James Crawford and Ian Brownlie, *Brownlie's Principles of Public International Law* (Oxford University Press 2019).

¹⁴ Teresa Scassa and Robert J Currie, 'New First Principles-Assessing the Internet's Challenges to Jurisdiction' (2010) 42 Geo. J. Int'l L. 1017.

¹⁵ Hamza Shahid, Meera Joshi and Mehmet Kaya, 'Cross-Border Data Flows and Conflict of Laws: A Multi-Layered Framework for Digital Trade Regulation' (2023) 2 Legal Studies in Digital Age 53.

operators. The physical basis of the digital companies is often lacking in the jurisdictions from which the companies are subject to regulation, making it difficult to make them comply with domestic regulation.

2.4 Public and Private International Law Perspectives

There is a public international law and private international law element to regulating cross border digital media. Jurisdictional issues relate to a public international law point of view the distribution, between sovereign states, of the powers of regulation. In this context, concepts like digital sovereignty, territorial powers and limits of territory, cyber governance, and international cooperation are present.

Private international law, on the other hand, is concerned with which rules and forum ought to be applied in conflicts between private parties involved in actions involving transnational activities. As the Internet providers become more involved in the legal obligations of the Internet, questions arise about the proper system of law to govern a specific case, such as issues of defamation, privacy, copyright or contract issues, as well as platform liability. Ensuring uniformity in national laws can create uncertainty and make litigation more difficult.¹⁶

They have been a new dimension in discussions of the regulation of online international platforms this not only by states but especially by private operators carrying out transnational online activities. As such, the public and legal systems have called for laws that can accommodate state jurisdiction in the context of a digitally connected world. It is less just a technical challenge and more one of the structures, as we have to think of jurisdictional arrangements in a world in which information does not occur within geographic boundaries.

Conceptual background outlined above illustrates that the legal landscape associated with transborder digital media is an interjurisdictional space of overlapping jurisdictions, conflicting

regulatory ends and a changing concept of sovereignty. These developments serve as a foundation for a discussion of some of the issues of jurisdiction facing international law in the digital era.

3. Jurisdictional Challenges in Cross-Border Digital Media Regulation

The recent development of cross-border digital media has revealed shortcomings in the status quo of territoriality. In fact, the domestic concept of territoriality has been exposed as being defective in the new reality of trans border digital media. International law offers principles for centralization and de-centralization of regulatory authority between States, but these principles are rooted in a predominantly territorial context and are not sufficiently robust to meet the challenges of the digital environment with its ever-global nature and cross-border (de)centralized infrastructures and information streams. Among the new challenges facing the state are the determination of which “law” applies, how to enforce regulations, who is liable for what, and how to deal with conflicts over competing jurisdictional claims, all of which are increasingly required to be resolved as digital platforms become the center of political discussion, economic activity, and social interaction. Such problems have turned into a key issue of the current discussion on digital governance and international law.

3.1 Determining Applicable Law in Cross-Border Digital Media Disputes

The cross-border nature of the sector creates several important jurisdictional issues, one of which is to establish the legal system to which digital activities across the border should be subject. Typical litigations in the old economy have a well-defined geographical aspect, thus establishing a fairly easy basis for granting jurisdiction. Conversely, many cases dealing with digital media disputes have multiple jurisdictions.

¹⁶ Marco Giacalone and Paola Giacalone, ‘When Private International Law Meets Technology’ *Research*

Methods in Private International Law (Edward Elgar Publishing 2024).

Businesses, for instance, can use social networking sites in various jurisdictions, have their business registered in other countries, and can serve users located in many states by hosting their pages on different locations on servers that are under the jurisdiction of other states besides where the business is registered. There are also tricky issues on the table that involve defamation, privacy violations, hate speech, infringing on intellectual property or disseminating illegal content which state's laws should govern the behavior?¹⁷

This is especially an issue if the national laws or regulations vary significantly. What is legally considered political speech can be legally deemed as hate speech, misinformation, blasphemous speech or unforeseen in one legal regime, but not the others. As a result, the interpretation of legality of exactly the same content delivered by the court and regulators may strongly differ. Lack of international standards heightens uncertainty for users, platforms, and governments.

Private international law provides ways of establishing applicability of law, based on conflict-of-law rules, but they were not created to address the scope and complexity of digital communications. In common situations these interactions enable online content to freely reach a diverse audience worldwide, and rarely is there any clear link that suggests which jurisdiction has the closest relationship with the dispute to assert jurisdiction over it.¹⁸

3.2 Extraterritorial Regulation and Conflicting Jurisdictional Claims

Digital media is ubiquitous worldwide and the international dimension of states' usage of digital media is now reflected by globally present extraterritorial jurisdiction. Nowadays, digital media is everywhere in the world, as is the extraterritorial dimension reflected in states' digital use. The trend is an acknowledgment that actions on the Internet, which come from outside

the country can have far reaching effects on a State's social, political, economic and security life, within that State's borders.

One instance of an extraterritorial regulation is the European Union's General Data Protection Regulation (GDPR). The GDPR extends beyond just those organizations based in the European Union, and strikes a blow at any organization located outside the EU processing the personal data of EU residents. There have been parallels in other fields, including online content moderation, competition policy, cybersecurity and online taxes.¹⁹

While there are advantages to extraterritorial regulation to increase the impact of domestic regulations, there are also disadvantages in terms of competing jurisdictional claims creating conflict. The laws concerning the same digital platform may conflict across various states. Laws in various states might overlap and conflict with one another. Under the current and proposed rules, a company might need to remove material from a nation's database in one country, but be covered by a constitutional free speech protection in another country. So the current and proposed rules mean that a company can find itself having to remove material from one database, while in another it is protected under a constitutional free speech provision.

In an era of more and more reliance on measures taken elsewhere, concerns have arisen about the possibility of regulatory fragmentation and the formation of a "splinternet" in which different parts of the world establish different and potentially incompatible regulatory regimes around digital communication technology.²⁰

3.3 Platform Liability and Accountability

Questionable liability of the platform is also one of the key jurisdictional issues. Digital platforms have a special role in the information ecosystem. They have made it clear that they are not

¹⁷ Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013).

¹⁸ Austen Parrish, 'The Effects Test: Extraterritoriality's Fifth Business' (2008) 61 Vand. L. Rev. 1455.

¹⁹ Lee A Bygrave, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020).

²⁰ Anupam Chander and Uyên P Lê, 'Data Nationalism' (2014) 64 Emory LJ 677.

publishers, and should not be considered such with regards to content created by their end-users. There are different ways being handled by different jurisdictions. Section 230 of the Communications Decency Act offers general immunity to online intermediaries' transmission of user-generated content in the United States. The Digital Services Act adopted by the European Union, however, sets higher requirements with regards to content moderation, transparency and risk management. Other nations, however, have implemented more stringent regimes, including the Chinese approach and others, that focus on greater government control and on the platforms' strong sense of responsibility.²¹

The challenge and difficulty of implementing these alternative legal options is compounded in the global activities of digital platforms. An international platform might set up reasonable expectations across various regions and jurisdictions around the globe regarding content, information integrity, expression and content-driven politics, hate speech, or privacy and other issues. A judicial enigma that exists with the conflicts is which country's laws shall take precedence in deciding the issue, especially if content is being viewed in a country, even if it is a country with a foreign dowager. One of the difficulties is that when content is being viewed in a country, even another foreign country as a dowager, which country's rules should take precedence.

In addition, content moderation moves are increasingly taken by the digital platforms are taken by automated application and artificial intelligence algorithm. Such transnational consequences have many implications beyond accountability, due process and judicial review at many levels.

3.4 Cross-Border Digital Evidence and Investigative Jurisdiction

²¹ Giovanni De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (Cambridge University Press 2022).

Problems of jurisdiction are also central issues when it comes to electronic evidence. When the police or security services are trying to investigate crimes committed online, cyberbullying, misinformation campaigns, terrorist propaganda or any other illegal activity online; they will need to access the data which is stored electronically, but not filed on their own territory.

But often there are legal and diplomatic hurdles to obtaining such evidence. Information pertaining to an investigation can be spread out over servers in various countries with differing laws and privacy, surveillance and disclosure requirements. Mutual legal assistance treaties (MLATs), which are often delayed and are out of pace with today's digital investigations, are frequently relied upon to access the digital evidence.²²

These questions have become more difficult with the advent of cloud computing. The information in the digital form may not reside in one identifiable place permanently, but rather move around dynamically in a global network of servers. Hence the location of evidence (and what state has authority over it) is not easy to determine in an increasingly complex way.

Investigative jurisdiction is thus an autonomous sector of the international law, becoming a subject of concern in international law. States want to be able to access the digital evidence from cross-border cases, while at the same time ensuring respect for foreign sovereignty and privacy rights issues. One of the hardest aspects of modern running of digital governance are balancing all of these different interests.

3.5 Content Moderation and the Enforcement Gap

Perhaps the most obvious territorial conflict in the governance of cross-border online media is due to content regulation. Governments are increasingly demanding digital platforms to remove content they consider to be harmful, unlawful and/or may

²² Robert J Currie, 'Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the "next Frontier"? (2017) 54 Canadian Yearbook of International Law/Annuaire canadien de droit international 63.

impair public order. But there are other rules and regulations surrounding 'content moderation' in different regions of the world.

If certain information concerns political dissent, religion criticism, historical interpretation or public morality, for instance, a different treatment could be applied based on domestic legal and or cultural context. Therefore, having to deal with a complicated environment of diverging legal requirements and social norms on a global level, platforms must face these considerations. Platforms operating worldwide must thus tread a tricky path between different sets of laws and expectations and social norms.²³

If they do manage to obtain jurisdiction and are able to issue lawfully binding orders, enforcement is still an issue. Conceivable that many digital "platforms" wouldn't have much or nothing to show for in the territories trying to control them. This also means that the regulatory decisions that are made may prove impractical to get colleagues to accept compliance with.

However, it is also very large in developing nations, in which regulatory institutions might not have the technological expertise to enforce effectively and/or have limited power when entering into negotiations with technology firms from other countries. Pakistan has encountered problems on occasions to implement the content restrictions and secure co-operation of foreign platform operators. Same problems have been encountered worldwide, on another continent, such as Africa and Asia.

This has led to a push for greater international collaboration as well as joint agreement on standards for international cross-border media regulation. If jurisdictions don't coordinate more, conflict over jurisdiction will grow as regulators extend their powers to the cyber realm, and new conflicts will be added to the former "digital poker face. If the jurisdictions don't coordinate more, jurisdictional disputes are likely to follow as jurisdictions extend the reach of their regulatory

powers to the cyber realm and new conflicts will be added to the former "digital poker face".

To sum up, there are deep jurisdictional issues regarding laws to be applied, certain aspects of regulation that affect content that goes beyond borders and the liability for the platforms as well as digital evidence and content moderation. The challenges highlight the weaknesses and outdated nature of classical legal principles of jurisdiction and underscore the need for novel legal concepts and mechanisms to confront the era of the interwoven digital frontier. The following section is devoted to the efforts by the key jurisdictions such as the United States, the European Union, China and India to address these challenges with their own regulatory frameworks.

4. Comparative Regulatory Approaches: United States, European Union, China, and India

Cross-border digital media has generated jurisdictional problems that has encouraged states and regional groups to take action with their own regulatory approaches. These methods have roots in the varying constitutional heritage, governments, economies and ideas of sovereignty. A number of jurisdictions focus on freedom of expression and market innovation, while others look to enhancing national security, public order, data control and creating digital sovereignty. This leaves the existing global system for regulating digital platforms with jurisdiction in more than one country - and often in different jurisdictions - with conflicting duties. An analysis of the ways the United States, the European Union, China, and India respond to digital media governance offers an illustration of how the governance of digital media relates to international law.

4.1 The United States: Market-Oriented Regulation and Freedom of Expression

Historically, the U.S. has taken a relatively "King's Court" stance on regulating digital media, and, at least in part, this perspective is grounded in the country's constitutional protections of freedom of

²³ Molly K Land and Jay D Aronson, *New Technologies for Human Rights Law and Practice* (Cambridge University Press 2018).

expression. Particularly helpful in protecting against government interference with freedom of expression, the First Amendment to the U.S. Constitution has had a profound impact on the doctrine of the Internet.²⁴

Section 230 of the Communications Decency Act (CDA) of 1996 is perhaps one of the most impactful laws concerning digital media in America. Section 230 provides all user-generated content sites with strong protection from liability (except where there is an obvious infraction of policies set by the platform provider) in exchange for their ability to filter out content they consider objectionable. The framework has been credited to helping the growth of digital platforms and to mitigate the legal risks from user-generated content.²⁵

Generally speaking, the system of American government and control relies on private mechanisms and self-government. Digital platforms have a lot of leeway when it comes to formulating community regulation, content moderation policies and enforcement policies. Government intervention is normally limited to specific situations such as criminal activity, violation of intellectual property rights, national security or other specific and narrow circumstances.

But, the U.S. system has been growing in disrepute in recent years. There have been worries about misinformation, online extremism, election manipulation, Internet hate speech, social-media platform monopolies and more, leading to demands for stricter regulation. And though there have been debates on these issues, the U.S. position is still rather conservative in terms of broad measures of content regulation and of any new or heightened intermediary liability requirements on digital platforms.

The American model has also been found to run counter to other regulations such as those used in certain countries from outside the U.S., especially as foreign governments attempt to have content taken away for which they deem protection necessary under U.S. constitutional requirements. The tensions here serve to highlight the difficulties of balancing values within a home country's constitution with a sense of the global realities of digital communication.

4.2 The European Union: Rights-Based Digital Governance

The EU is more sensitive to the balance between freedom of expression and privacy, consumer protection, accountability and fundamental rights than the USA.

Perhaps most importantly, there was the General Data Protection Regulation (GDPR) which took effect in 2018. The GDPR is the exhaustive set of rules controlling the data collection, data sharing, and data processing with regards to personal data. Notably, it is not limited to EU countries, but extends to organizations based outside of the EU that process information on EU citizens. This has resulted in the GDPR being one of today's most significant cases of jurisdictional extension in the digital age.²⁶

In addition, the EU has tightened up on regulations independently with the Digital Services Act (DSA) and Digital Markets Act (DMA). The DSA will obligations for platforms ensured transparency, risk evaluations and assessment, illegal content deletion, user safeguards. Meanwhile, the DMA is aiming to rein in competition worries, including over the dominance of big so-called digital gatekeepers with a heavy (or disproportionate) footprint in online markets.²⁷

²⁴ Erwin Chemerinsky and Jesse H Choper, *Constitutional Law: Principles and Policies* (Aspen Publishers New York 2006).

²⁵ Jeff Kosseff, *The Twenty-Six Words That Created the Internet* (Cornell University Press 2019).

²⁶ Paul Voigt and Axel Von dem Bussche, 'The Eu General Data Protection Regulation (Gdpr)' (2017) 10

A practical guide, 1st ed., Cham: Springer International Publishing 10.

²⁷ Tiago Morais Rocha, 'Digital Services Act: Towards the Digital Rule of Law' *International Conference a Digital Europe for Citizens, Data governance, Digital Markets, Digital Services* (Springer 2023).

One of the peculiar characteristics of the EU model is that it places a strong emphasis on the protection of fundamental rights. Privacy and data protection are two fundamental rights granted to individuals that are recognized in European jurisprudence and are afforded the strongest possible legal protections. Thus, digital services dealing with the European market would be under more extensive regulation than would be applied under the American model.

European regulatory developments have had an impact on the worldwide regulations, commonly called the "Brussels Effect. Furthermore, the EU directives and practices often extend beyond their European area of operation and impact multinational corporations which seek to enter that EU market, thus leading to GDPR appropriate global operating practices in practice.²⁸

4.3 China: Cyber Sovereignty and State-Centric Regulation

China has a clear governance model for digital media that contrasts with others. Chinese digital regulation does not value openness nor deprecate transnational information flows but takes the principle of cyber sovereignty, which states their right to "full control" over events taking place within their digital spaces.²⁹

The Chinese model emphasizes the needs of state security, social stability and information-control by the state. Authorities in China have implemented a high degree of regulatory leverage across digital platforms and online content through legislative, technical and administrative means.

The Cybersecurity Law, the Data Security Law and the Personal Information Protection Law (PIPL) are part of China's regulatory regime. Taken together, these laws outline data localization, compliance with cybersecurity, content regulation and cross-border data transfers. Almost always, all foreign companies doing business in China will be

bound by stringent data governance obligations and may even need to keep some types of data at the Chinese location.³⁰

The Chinese way goes through intensive obligations of content moderation from digital platforms. It expects service providers to monitor content for proactively removing service content that is deemed to be unlawful or harmful to State interests. This reflects in stark contrast to regulatory approaches in the United States and other liberal democracies that are more liberal.

Discussions about the Chinese model focus on freedom of expression and access to information; the detractors doubt it's free and the defenders say that it's often a legitimate exercise of state sovereignty in the digital world. In some developing nation-states that want to extend their control of the infrastructure and flows of information, the idea of "cyber sovereignty" has become influential.

4.4 India: Balancing Digital Growth and Regulatory Control

India is in a unique place in the world of digital governance. India is one of the largest online markets in the world and has been challenged with the need to keep pace with rapid growth in the online market while simultaneously addressing concerns related to national security, misinformation, data protection and public order. In recent years, Indian authorities have increasingly embraced a heavy-handed stance against digital media because of a number of issues. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 imposed new duties on social media intermediaries along with enhanced guidelines on content moderation, grievance redress mechanisms and assistance provided to law enforcement agencies.³¹

India has also been taking proactive steps to enhance data governance by enacting the Digital

²⁸ Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020).

²⁹ Samantha Hoffman, 'Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion'.

³⁰ Douglas W Arner, Giuliano G Castellano and Ėriks K Selga, 'The Transnational Data Governance Problem' (2022) 37 Berkeley Technology Law Journal 623.

³¹ *ibid.*

Personal Data Protection Act 2023 (DPDPA), which introduces laws on personal data processing, consent and data protection requirements. While it is not exactly the GDPR, this piece of legislation shows there is increased awareness of concerns around privacy and data governance in India's digital economy.

One particular aspect of Indian thought is that they make a concerted effort to balance competing demands. On the other, the idea is to foster innovations, foreign investment and technological advancement. In the other, they highlight the need to assert the state's power over online content and the threat from misinformation, public disorder and national security in the online space.

India's regulatory strategy thus falls in between the relatively liberal U.S. approach and the more 'state centric' strategy of China. How to connect competing visions of digital governance?⁴ How to relate to competing visions of digital governance?

4.5 Comparative Analysis: Competing Visions of Digital Governance

It is clear from the differences between these four jurisdictions that both notions of governance and jurisdiction differ from state to state when it comes to digital media. The constitution of the United States advances a commitment to limited governmental interference in speech with focus on freedom of speech and intermediaries, or middle-man's, immunity. It is under this light of rights-based regulation that the European Union focuses on privacy, accountability and platform responsibility. China's policy is to have a model of sovereignty where state control and national security are paramount, and India wants a mix of digital innovation with increasing measures of regulatory oversight.³²

The conflicting approaches pose major difficulties for international law. Multinational Digital Platforms should fulfill different legal conditions that can even be conflicting in various countries. What is okay in one jurisdiction is not necessarily

in another and what is okay to transfer in one regulatory regime may be not okay in another's privacy laws. As a result, the world has become more and more fragmented in digital realm.

The comparative analysis also reveals the fact that jurisdictional debates in the field of digital medias governance are not only legal technicalities about legal abilities. They express more fundamental conflicts between nations over sovereignty, around human rights, over democracy and about what is to be done with technology. The need for more cooperation, more harmonization of the regulatory efforts is growing with the expansion of States' regulatory powers in cyberspace.

5. Digital Sovereignty, Human Rights, and International Law

Then, more than one issue is about competence; it's also about the balance of norms (state sovereignty and internationally recognized human rights) in cross-border digital media regulation. With the increasing infiltration of digital communication in the political, economic and social sphere, there is growing conflict between efforts by the State to regulate digital environments and claims to fundamental rights with respect to freedom of information, privacy and freedom of expression. However, there is partial framework for resolving such tensions in international law, which is, in the digital space, somewhat fragmented and controversial.

5.1 Digital Sovereignty and the Reassertion of State Control

Digital sovereignty is defined as the sovereignty of states over digital infrastructure, flows of data, platforms and information spaces that occur within these territories. In practice it embodies an extension of the traditional concept of sovereignty to cyberspace, where states try to control not only domestic actors but also foreign technology companies that use or impact their cyberspace.³³

³² Maseeh Ullah, Muhammad Haris and Najeib Ullah Khan, 'Data Governance and Cross-Border Flow Regulations: A Comparative Study of China's FTAs

and WTO Framework' (2025) 3 The Critical Review of Social Sciences Studies 1404.

³³ Ronald J Deibert, *Reset: Reclaiming the Internet for Civil Society* (House of Anansi 2020).

Questions of data security, foreign surveillance, platforms' dominance and informational influence are conspicuously intertwined with the concept of digital sovereignty. The importance of digital infrastructure in today's society has increased and is becoming increasingly a strategic asset for various states to look into, especially as they consider national security and economic independence. The result of this has been laws and rules like data localization, controls on data transfers across borders, and tight regulations around digital platforms.

There are also fragmentation concerns in the international Internet, however, which digital sovereignty brings with it. The level of attention on national control can increase the risk of the 'splinternet' – where the internet is split into multiple sections with different regulatory frameworks and different laws. This "fissioning" can challenge the openness and interconnection of digital communication networks.³⁴

5.2 Freedom of Expression in Cross-Border Digital Media

The fight for freedom of expression is among the most debated one among others that are being fought in the regulation of digital media. The right to find, receive and share information across borders is guaranteed by international law, including Article 19 of the International Covenant on Civil and Political Rights (ICCPR). More relevant for the digital atmosphere, where information flows are seen as a constant happening across borders.³⁵

Digital covers opened up opportunities for expression by facilitating participatory public discourse around the world. But they also have introduced fresh regulatory problems, especially with regard to politically sensitive speech and the dissemination of hate speech, extremism and misinformation. States are often found restricting

access to online information in the name of public order, national security or, morality.

The main challenge in law is whether any such restrictions are justifiable and proportionate in terms of international human rights law. Although there are specific restrictions on free expression allowed under international law, they are required to meet stringent conditions of legality, necessity and proportionality. However, it needs to be noted that in practice states have different interpretations of these requirements, and that this might result in unfavorable differences in the level of regulations in individual states. But in practice, different interpretation of the requirements means different regulatory outcomes may be seen from jurisdiction to jurisdiction.³⁶

5.3 Privacy, Surveillance, and Data Protection

SOA privacy is one of the biggest human rights issues in the digital era. Today, an increasing number of individuals give their personal data to digital platforms and receive in return user-friendlier services, while corporations and states contribute revenue sharing to culture and the privacy of their citizens. Rather, the contribution of personal data from individuals, its processing by corporations, its monetization by capitalists, and the services provided to the user has revolutionized the relations between individuals, companies, and states. The protection of privacy is further complicated by cross-border data transfers, and in many jurisdictions, personal data is held in more than one jurisdiction, where the protection of privacy may be different.

Privacy is a fundamental human right that is recognized by International human rights law outlined in Article 17 of ICCPR. But, privacy protections in digital environments are not always in place. In some countries—like the European Union—there are extensive data protection

³⁴ Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020).

³⁵ Linda Camp Keith, 'The United Nations International Covenant on Civil and Political Rights:

Does It Make a Difference in Human Rights Behavior?' (1999) 36 *Journal of Peace Research* 95.

³⁶ Md Nurul Momen, 'Myth and Reality of Freedom of Expression on the Internet' (2020) 43 *International Journal of Public Administration* 277.

regimes, but a few others adopt information field-by-field or fragmented ones.³⁷

State surveillance practices also raise significant concerns. Governments increasingly rely on digital technologies for intelligence gathering, cybersecurity monitoring, and law enforcement. While such practices may be justified on security grounds, they must be balanced against individual privacy rights. Excessive surveillance, particularly when conducted across borders, raises questions of legality and accountability under international law. There are also serious concerns about the practices of state surveillance. Digital technologies have become an integral part of governments' capabilities to collect intelligence, monitor cybersecurity, and track criminals. Though it may be required on security concerns there must be balance between these and the rights of individuals. No one wants more surveillance and especially not when it's crossing borders: questions of legality and accountability arise internationally.

5.4 Human Rights and Platform Governance

It is digital platforms that are now defining what is permissible speech and what information can be accessed. Platforms exercise quasi-regulatory authority via penalties, rankings, and automated enforcement systems, within the context of the rules and policies they set. Content moderation policies, algorithmic ranking systems, and automated enforcement systems allow platforms to effectively perform quasi-regulatory functions. This has called into question their obligations to respect national and international human rights norms.

There is growing scholarly and policy interest in and awareness that there are obligations for private online platforms in relation to human rights, in addition to states. The United Nations Guiding Principles on Business and Human Rights (UNGPs) reinforce this concept of

corporate responsibility, which calls for due diligence, transparency and accountability.³⁸

These principles are challenging to apply however, due to the transnational nature of platform operations. Platforms face the challenge of meeting multiple state laws with varying definitions about what can and cannot be found on the platforms and about individual user rights. This results in the existing environment being a complex governance context where protection of human rights may differ greatly from territory to territory.

5.5 Pakistan's Perspective: Surveillance, Cybercrime, and Digital Rights

The digital sovereignty and human rights and the cross-border media regulation may pose severe institutional and legal hurdles in developing jurisdictions like Pakistan. The major legislation covering cybercrime offences, content controls and Digital enforcement is the Prevention of Electronic Crimes Act (PECA) 2016. Its use in other jurisdictions, meanwhile, presents some challenging issues, especially if the digital platforms and servers are situated abroad.

The conflict between regulating for surveillance and constitutional rights to privacy and freedom of expression in Pakistan's digital regulation regime have been discussed in recent scholarly writings. Specifically, by scholars prof. Michael D'Antoni, who argue that, although digital surveillance systems are to be used to better protect cybercrime and national security, public safety policies should not be expanded to the extent that they threaten international human rights obligations or offer constitutional protections.³⁹

In addition, PECA has enforcement challenges with respect to cybercrime: Enforcement of PECA is transnational because cybercrime is transnational. Identity theft, Internet frauds, and data breaches are some of the crimes that often

³⁷ Lee Andrew Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press 2014).

³⁸ John Gerard Ruggie, 'The Social Construction of the UN Guiding Principles on Business and Human Rights' *Research handbook on human rights and business* (Edward Elgar Publishing 2020).

³⁹ Muhammad Faiq Butt and others, 'THE RIGHT TO PRIVACY IN THE AGE OF SURVEILLANCE: LEGAL PROTECTIONS IN PAKISTAN' (2024) 2 ASSAJ 1449.

have actors and infrastructures in several jurisdictions. This leads to gaps in enforcement as the domestic laws and bodies do not provide adequate security for foreign cooperation or for collecting evidence on the internet across the border. Through Hashmi's scholarship, the importance of developing more robust cooperation mechanisms between countries and the incoherence of rules of jurisdiction was reiterated to deal effectively with the limits of enforcement.⁴⁰

But, in broader context, there is more of a challenge for the overall society on how to balance legitimate state interest in cybersecurity and public order with respect to a trade-off of fundamental rights in a digitally interconnected society. This involves not only the need for internally reforming the law but also adapting to new international best practices and standards in data protection, cyber governance and platform accountability.

5.6 Normative Tensions in International Law

The many facets of digital sovereignty and human rights highlight a basic conflict between two norms in international law. On the other hand, states are claiming that they can control their digital environments to secure, develop the economy and stabilize society. However, international human rights law places limits on the power of the state, as it does in regard to expression, privacy and access to information.

This tension is made worse because there is no one set of guidelines worldwide in regards to digital media regulation. This has made international norms a source of interpretation and implementation divergence amongst the states and ultimate legal uncertainty. There has been some convergence, which has appeared in the form of soft law agreements and through a regional regulatory approach, but there are still a lot of gaps.

The challenge in the end is to create an enablement of a governance model to incorporate

both state sovereignty and UHR within a technologically changing landscape. Increased efforts are needed to coordinate activities between countries and implement better accountability systems for digital platforms, to strengthen the embedding of human rights into digital governance in countries.

6. Pakistan's Legal Framework and Emerging Challenges in Cross-Border Digital Media Regulation

Regulation of cross-border digital media platforms in Pakistan has been a reactive and increasingly complex process, which has been influenced by the swift adoption of digital technology, skyrocketing reports of cybercrime, political debate over online speech, and the impact of foreign digital platforms. Although the state has established a formal legal architecture for cyber regulation, there are large jurisdictional, institutional and enforcement gaps that rely on foreign host platforms, cross-border data flows. These challenges illustrate some of the dynamics between sovereignty, constitutional rights, and international legal collaboration of the dramatic developments in cyberspace.

6.1 The Prevention of Electronic Crimes Act (PECA) 2016: Scope and Jurisdictional Reach

The cornerstone of the cyber regulatory regime in Pakistan is the Prevention of Electronic Crimes Act (PECA) 2016 which criminalizes a wide range of cyber related offences like "Unauthorized Access, Electronic Fraud and Offences against Financial Systems, Cyberstalking, Identity Theft, Data Interference and Distribution of Unlawful Mail. Significantly, PECA also contains an 'extraterritorial' clause, providing the authority for remediation of activities that are carried out outside of Pakistan involving persons, systems and data within the borders of Pakistan."⁴¹

This extraterritorial reach is intended to make laws more in line with the borderless digital activities.

⁴⁰ Sadia Nazir, Muhammad Asif and Asad U Allah Khan, 'Digital Evidence in Pakistan: A Doctrinal Assessment of Admissibility and Reliability in Criminal

Trials: <https://doi.org/10.55966/assaj>. 2025.4. 1.0107' (2025) 4 ASSAJ 1941.

⁴¹ Muhammad Iqbal and others, 'The Prevention of Electronic Crimes Act (PECA) 2016: Understanding

In practice, however, it is enforcement structures and arrangements that are heavily reliant on international cooperation, especially through mutual legal assistance treaties (MLATs), informal diplomatic channels, and voluntary cooperation of foreign technology companies. Given the lack of enforcement mechanisms for foreign parties, the role of PECA in transborder disputes over the Internet remains limited.

Further, there are some concerns over the interpretation of PECA's broad definitions, which sometimes have an ambiguous wording and scope, especially in the area of "unlawful content" and "glorification of offense." These ambiguities further add difficulty in the application of the jurisdiction, particularly for those whose content is published abroad but is made available to the users in Pakistan.

6.2 The Role of the Pakistan Telecommunication Authority (PTA)

Pakistan Telecommunication Authority (PTA) is also involved in regulating the digital media content as well as ensuring compliance amongst online platforms. In accordance with PECA and relevant regulations, PTA has the powers to block, restrict or delete online content that is illegal or detrimental to national interests.

In the past few years, PTA has been active and more active lately in engaging with world-class chatting sites like Facebook, YouTube, X (Twitter) and TikTok to request removal of content and regulatory compliance actions. But the interactions show how the point of eligibility is tilted in favor of Pakistan, as it would be difficult for the country to effectively enforce its laws over Internet service providers unless they were to sit in Pakistan's jurisdiction or actively cooperate in doing so.⁴²

This imbalance of rights is typical of international digital governance structures in general. The specific power in the digital market determines the possibility and influence of regulation by the state,

which depending on the market power may take the form of market access conditions with greater capacity to ensure compliance to those with smaller digital markets.

6.3 Cross-Border Data Flows and Digital Sovereignty Concerns

Turning to cross-border data flows is one of the important regions of concern for Pakistan's regulatory bodies. As an increasing number of businesses move everything to the cloud, host files elsewhere and upload their data to foreign storage infrastructures, concerns about how data will be controlled, how it will be protected, and how it will be kept secure abound.

Although there has been a draft bill of the Personal Data Protection Act for a number of years, Pakistan still has not enacted a comprehensive regime for the protection of personal data. With the lack of a finalized data protection law, regulatory answers to cross border transfers of data are limited and are frequently a matter of administrative judgment.

This loophole in the laws leaves room for uncertainty for users as well as service providers. Digital platforms with a Pakistani presence have to deal with ambiguous legal demands on data localization, user consent, and data transborder data flow. Meanwhile, the state's problems lie in ensuring this vulnerable personal data of its citizens is properly protected from Pakistani perpetrators while being processed and stored on foreign servers.

By contrast, other regions have implemented strong data transfer mechanisms in the GDPR and China has data localization regulations. The changing scenario in Pakistan shows that he has slipped in the globe's regulatory corridor, and Pakistani sovereignty-Related concerns are being amplified yet there is a lack of developing of institutional organizations in Pakistan.

the Challenges in Pakistan' (2023) 2 Siazga Research Journal 273.

⁴² Asad U Allah Khan, 'Cyber Crime in Pakistan: Trends, Challenges, and Legal Responses: <https://doi.org/10.55966/Assaj.2025.4.1.080>' (2025) 4 ASSAJ 1358.

Org/10.55966/Assaj.2025.4.1.080' (2025) 4 ASSAJ 1358.

6.4 Enforcement Challenges in Transnational Digital Contexts

Enforcement of the digital law in Pakistan is particularly difficult in the case of foreign registered platforms and actors. Most of the frequently used online platforms do not have significant physical presence in Pakistan and therefore judicial or administrative directions are not easily enforceable against them in Pakistan.

The Enforcement Gap is more pronounced in situations where online defamation, misinformation, hate speech and cyber fraud comes from outside the zone of regulation. Where Pakistani courts or regulatory bodies have ordered the removal of content or limitations on accounts are followed or not relies not on any solid international legal obligations, but on the company's internal policies.

Moreover, computer evidence used for demonstrating the perpetration of cybercrimes is often housed at foreign data centers. This gives rise to delays in procedure and obvious evidence hurdles because access to such information would normally be affected in advance by making such a formal request in accordance with the framework of the MLATs. These processes are typically clumsy, cumbersome and time consuming and do not meet the urgency of Internet crimes.

It is highlighted here that it is not a Pakistani draconic rule, rather this is seen in many developing legal systems in the world which operate amidst a digitally interconnected world.⁴³

6.5 Constitutional Rights, Digital Regulation, and Judicial Interpretation

Pakistan's constitution provides for the freedom of speech (Article 19) and privacy of home (Article 14) with reasonable restrictions under the law. As issues around online expression and surveillance play out in court and regulations bodies, the meaning of these rights is drawing more attention.

⁴³ Muhammad Mansur ALIYU and Kabiru Ibrahim ABDULKADIR, 'CYBERCRIME AND THE EXERCISE OF CRIMINAL JURISDICTION IN NIGERIA: A DOCTRINAL ANALYSIS' (2026) 7 INTERNATIONAL JOURNAL OF LAW AND CLINICAL LEGAL EDUCATION.

In general, judicial approaches have been aimed at reconciling constitutional freedoms and considerations with concerns of national security, public order and of sensitivities toward religion. But doctrinal developments have not kept up with the development of the various digital technologies, and constitutional interpretations know no uniformity.

Specifically, issues of proportionality and due process protections in the context of PECA have come into question. Critics say there is a risk that sweeping regulatory discretion will result in inconsistent enforcement, and in stifling online free expression. Meanwhile, cyber rule makers highlight the need for these measures due to attempted Internet misuse and misinformation.

6.6 Scholarly Contributions and Emerging Legal Perspectives

The recent research and scholarly work have been pivotal in dissecting the complex and evolving nature of Pakistan's legal landscape in the digital era, specifically concerning issues of cybercrime, surveillance, and territorial jurisdiction. They've studied digital privacy and surveillance and uncovered a "structural tension" between the increased capabilities of the government to monitor and constitutional protections of individual rights. In its argument, it considers surveillance mechanisms to be more justifiable to bolster cybersecurity and national security powers, but argues that a strong legal framework, judicial control and proportionality threshold are integral to the operation of those powers.⁴⁴

Furthermore, their cybercrime enforcement analysis includes the fact that Pakistan's legal system is greatly hamstrung in its ability to address cybercrime because of its overreliance on jurisdiction considerations. Some of these relate to challenges in foreign-stored digital evidence, absent a harmonized international cooperation

⁴⁴ Muhammad Faiq Butt and others, 'THE RIGHT TO PRIVACY IN THE AGE OF SURVEILLANCE: LEGAL PROTECTIONS IN PAKISTAN' (2024) 2 ASSAJ 1449.

mechanism, and inadequate enforcement ability against foreign intermediaries. The scholarship indicates that a country's response to these issues must involve not just national legislative adaptation, but also increased role-playing in international legal doctrines on cooperation in cyberspace. According to the scholarship, the response of a country to these issues should be the adoption of national legislation in addition to involvement in international legal frameworks on cooperation in cyberspace.⁴⁵

These submissions are important for the purpose that they put the issue of governance in Pakistan in the context of global discussions on issues of digital sovereignty, human rights and jurisdiction issues.

6.7 Concluding Observations on Pakistan's Digital Legal Regime

The cross-border digital media regulation regime in Pakistan seems to be in a transitional phase representing the evolution of cyber governance. PECA 2016 and linked regulatory mechanisms offer a initial framework, however there are a number of challenges in complying with the rules, offering certainty and guarding against incompatibility with world requirements.

At heart, the problem is the fundamental incompleteness of territorial and law-based concepts of legal jurisdiction and their relationship with digitally connected infrastructures. The problem is, at the core, territorial jurisdiction concepts and their corresponding legal systems are simply incompatible with digital technologies and their networked infrastructure. For as long as there is no uniform regulation of digital platforms where they are operated across multiple jurisdictions and do not have uniform obligations regarding their enforcement, gaps in enforcement and jurisdictional issues will remain a problem.

To solve these problems will require a mix of domestic legal reform, strengthen the institutional capacity and deepen international cooperation. Especially, a comprehensive data protection

regime, proper jurisdictional provisions, and better cross-border enforcement mechanisms will play a vital role when it comes to building a digital governance system in line with global standards in Pakistan.

7. Towards a Harmonized International Framework for Digital Media Governance

The diversity of laws and policies across various EU member states regarding transborder digital media has intensified efforts to create a more coherent and harmonized international approach. Unilateral strategies, whether rights-based, sovereignty-based or market-oriented, have been found to result in conflicting jurisdictions, gaps in enforcement and conflicting norms as shown in the previous section. International law is currently up against this issue of balancing state sovereignty with the "transnational" nature of digital communication. A harmonized framework should be neither intended to eliminate national regulatory diversity nor designed to define a universal allocation of jurisdiction in the cyberspace, but should establish minimum standards, procedures, and principles for the allocation of jurisdiction in cyberspace.

7.1 The Need for International Cooperation in Digital Governance

Digital media are international and so are the means of international communication, meaning that unilateral regulation is structurally inadequate. Information from one jurisdiction is immediately available for the whole world and digital platforms run multi-jurisdictional to function across the various jurisdictions. This interdependence must be reflected on how to establish and operate coherent governance arrangements that can address disputes and conflicts across the border.

Cybercrime, misinformation, data protection and platform accountability are areas in which collaboration is vital on a global scale. The current tools, such as mutual legal assistance treaties (MLATs), are appearing to be the wrong tools

⁴⁵ Hafiz Abdul Rehman Saleem and others, 'Challenges Faced by the Judiciary in Implementing Cybersecurity

Laws in Pakistan' (2025) 3 The Critical Review of Social Sciences Studies 1052.

today because of delays, complexity and jurisdictional hurdles. Scholars have consequently underscored the importance of streamlined cooperation frameworks which will enable quicker and more efficient cross-border data sharing as well as of assistance regarding enforcement. Scholars have therefore emphasized the need for simplified cooperation structures which will support speedy and efficient cross-border data sharing on the one hand and provisions of cooperation on the side of enforcement on the other.⁴⁶

A single framework would also simplify compliance with the legal obligations faced by all digital platforms, which currently have to deal with conflicting obligations as between jurisdictions. Without effective coordination, companies end up having to implement what it's called "regulatory over-compliance": whether in a distributed way or as a unified approach, these companies adopt the most stringent legal standard anywhere in the world, which can negatively impact local freedoms and legal pluralism.

7.2 The Role of the United Nations and Global Institutions

The Internet has been identified as a major arena in which there are discussions regarding internet governance and digital regulation within the United Nations system. There are no binding treaties at the global level that regulate digital media, although several UN agencies such as the Human Rights Council, the Internet Governance Forum (IGF) and the International Telecommunication Union (ITU) have played a role in the process of norm building and policy coordination.

The UN Human Rights Council has especially reaffirmed that the same rights that apply to the offline world must also be respected online such as the right to freedom of expression and privacy rights. Normative implications of this principle remain, however, with no enforceable

mechanisms in place, it is not very impactful practically.⁴⁷

The IGF is a multi-stakeholder forum that convenes representatives from governments, technical community, civil society and the private sector. It is not binding, but it has a strong influence on the international debate on regulating the internet and helping to build international consensus.

Extension of UN involvement in digital governance may lead to a more robust international framework, but to date this has not happened and may be manifest as a 'framework convention on digital governance'. The instrument could define the principles, standards and requirements for data protection and the commitments for cooperation at a baseline level and offer flexibility in national implementation of the instrument.

7.3 Emerging Models of Digital Governance Treaties

There are a few conceptual frameworks for the international agreement that will have to emerge to tackle digital governance issues. There are a number of ideas from lawyers about how an international agreement might work to solve digital governance problems. The proposals tend to be limited to the key areas of determining the rules for which jurisdiction applies, cross-border data transfers, platform responsibility, and the rule of content moderation.

One route is to build up harmonization standards that would define the minimum level that ensures the autonomy of the individual States' policies but yet share in common certain principles. A second proposal proposes using mutual recognition approaches, which involve outreach or agreement between states to validate and respect specific digital regulation regulations adopted from other jurisdictions under specific circumstances.

The Budapest Convention on Cybercrime is one of the most important instruments on the international level in this regard. It offers

⁴⁶ *ibid.*

⁴⁷ Ahreum Lee, 'International Human Rights Law in Digital Space: An Examination of the Need for New Legal Measures for the Protection of Rights Online'.

guidelines for cooperation in the investigations and prosecutions of cybercrime and offers procedural suggestions for access to data from international jurisdictions. The lack of membership and a focus mainly on criminal issues, however, limit its usefulness in a wider context relating to governance in digital media.⁴⁸ More contemporary past deliberations have addressed the idea of a “Digital Geneva Convention” to govern national actions in cyberspace, especially on the matter of cyberspace action, digital infrastructures’ protection, and governance of platforms. Although these ideas are yet on paper, they herald a new awareness of the need for an overall international legal framework.

7.4 Multi-Stakeholder Governance and Private Actor Participation

One aspect that is very typical of digital governance is the prominence of private actors, especially the multi-national tech giants. A digital platform can fill quasi-governmental roles in several ways, such as content moderation, algorithmic ranking, and systems of user governance, as opposed to traditional regulatory environments.

Hence, there is no possibility that this regulatory system can be exclusively state based at the international level. In this context, a multi-stakeholder governance model is becoming a necessity to tackle complexity in digital ecosystems. This Model includes working together between Governments, private companies, civil society, technical communities and international institutions.

Private platforms already engage in informal governance globally by observing national legislation, by implementing voluntary options to delete content and by entering into consultation processes with the regulatory bodies. International legal obligations, however, are restricted for them. Improving transparency commitments, due process rules, compliance with human rights norms for digital platforms can reinforce the legitimacy of the governance.

7.5 Future Directions: Toward a Coherent Digital Legal Order

A juxtaposition between fragmentation and harmonization is likely to be important for the future of cross-border digital media regulation. States on the other hand are making a strong case for a digital sovereignty, with varying levels of regulations instituted. Conversely, the digital communication's interconnectedness leads to significant incentives for convergence and cooperation.

Any attempt to establish an international digital legal order would probably need a number of bases. First of all, it is important to develop clear jurisdictional rules to prevent conflicts of law and multiple regulatory claims”. Second, the principles need to be standardized for more efficient enforcement, in order to access and share data from other jurisdictions. Third, there should be an improvement of minimum standards for globally protecting human rights in digital environments, so as to guarantee uniform protection of freedom of expression and privacy rights.

If the digital ecosystem doesn't change then it could continue to have even more fragmentation, uncertainty in regulation and unequal results of the enforcement. This may disadvantage structural disadvantages in the implementation of any action by the digital measures by the states in developing countries before the powerful ones of a transnational nature.

International law itself must move beyond its concepts and claims based on territory to more flexible, mutually collaborative and technologically responsive methods in this context. However, this is not simply a challenge of control, but one of building an information governance system that protects rights, is open and is effective in a borderless information environment.

Conclusion

The regulation of trans-border Internet media is one of the most intrinsically complicated areas of current international law. The study conducted in this paper already shows that the traditional legal

⁴⁸ ibid.

principles such as territoriality, nationality and effects are coming under strain as a result of the borderless structure and openness of digital communication. Social media, cloud systems and algorithmic information systems are transcending legal systems and leading to concurrent jurisdiction claims and frequent conflicts of law.

The research has revealed that jurisdictional uncertainty poses the greatest threats in four interrelated areas: choice of law, attempts to assert jurisdiction out of border, platform liability, and enforcement of digitally collected evidence across borders. Added to this, there are now vastly different philosophies about how to regulate by major jurisdictions. In the U.S. emphasis is placed on intermediary immunity and on expressive freedom; the EU attaches importance to the rights perspective and a compliance regime; China is based on a sovereignty principle and a rule of control; and India has a combined development-oriented regime with growing state control. This separation has helped to create what could be called a confused digital constitutional structure, which imposes provisional or various differences in the legal obligations based on the local context in which the rule is to be applied.

The study at a normative level state that the ongoing conflict between digital sovereignty and universal human rights is a priority. States are increasingly claiming regulatory powers in digital ecosystems to safeguard security, public order, and cultural integrity but do so at a time when key internationally-recognized fundamental rights, such as freedom of expression and privacy, actively oppose that regulatory control. These tensions have been compounded by the lack of common global law format and are dependent more and more on soft law tools, bilateral agreements and corporate self-regulation.

The detailed consideration of these broader trends in the Pakistan context also helps to clarify how they play out in the developing legal system. While PECA 2016 and the related regulatory instruments offers a legal framework for cyber governance, some inherent weaknesses may hinder the effectiveness of regulations, including limitations in the enforcement capability, jurisdictional interferences, and reliance on

compliance of foreign platforms. The scholarship of Muhammad Ahsan Iqbal Hashmi and co-authors supports the idea that Pakistan's legal approach to the Internet and other technology-driven, cross-border activities is a global challenge: how to enforce territorially-based legal systems in a way that safeguards constitutionally guaranteed fundamental rights and promotes procedural fairness for all parties involved.

At the end of the study, it is concluded that there is a need for incremental adjustments in present runways, rather than any "brand new" frameworks. There needs to be a more coherent international approach that brings together minimum jurisdictional standards and enhances cross-border cooperation mechanisms and incorporates protection of human rights into the design of digital governance. Politically and legally complex issues will need to be faced in reaching full harmonization, but greater convergence through multilateral agreements, platform accountability regimes and interoperable regulatory techniques seems both possible and desirable.

Summarizing, the subject of a cross-border digital media had completely reshaped the concept of the relationship between law, sovereignty and communication. International law has thus to move beyond strictly territorial notions and embrace more flexible, collaborative, and technologically-friendly models of lawmaking for a world increasingly inhabited by networks and networks of networks if it is to maintain the certainty of law, secure rights, and assure the effectiveness of regulation in the digital age.

References

- ALIYU MM and ABDULKADIR KI, 'CYBERCRIME AND THE EXERCISE OF CRIMINAL JURISDICTION IN NIGERIA: A DOCTRINAL ANALYSIS' (2026) 7 INTERNATIONAL JOURNAL OF LAW AND CLINICAL LEGAL EDUCATION
- Arner DW, Castellano GG and Selga ĖK, 'The Transnational Data Governance Problem' (2022) 37 Berkeley Technology Law Journal 623

- Bradford A, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020)
- , *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020)
- Butt MF and others, 'THE RIGHT TO PRIVACY IN THE AGE OF SURVEILLANCE: LEGAL PROTECTIONS IN PAKISTAN' (2024) 2 ASSAJ 1449
- , 'THE RIGHT TO PRIVACY IN THE AGE OF SURVEILLANCE: LEGAL PROTECTIONS IN PAKISTAN' (2024) 2 ASSAJ 1449
- , 'THE RIGHT TO PRIVACY IN THE AGE OF SURVEILLANCE: LEGAL PROTECTIONS IN PAKISTAN' (2024) 2 ASSAJ 1449
- Bygrave LA, *Data Privacy Law: An International Perspective* (Oxford University Press 2014)
- Bygrave LA, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)
- Chander A and Lê UP, 'Data Nationalism' (2014) 64 Emory LJ 677
- Chemerinsky E and Choper JH, *Constitutional Law: Principles and Policies* (Aspen Publishers New York 2006)
- Crawford J and Brownlie I, *Brownlie's Principles of Public International Law* (Oxford University Press 2019)
- Currie RJ, 'Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the "next Frontier"?' (2017) 54 Canadian Yearbook of International Law/Annuaire canadien de droit international 63
- De Gregorio G, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (Cambridge University Press 2022)
- Deibert RJ, *Reset: Reclaiming the Internet for Civil Society* (House of Anansi 2020)
- Giacalone M and Giacalone P, 'When Private International Law Meets Technology' *Research Methods in Private International Law* (Edward Elgar Publishing 2024)
- Goldsmith J, 'Who Controls the Internet? Illusions of a Borderless World' (2007) 23 Strategic Direction
- , 'Who Controls the Internet? Illusions of a Borderless World' (2007) 23 Strategic Direction
- Hoffman S, 'Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion'
- Iqbal M and others, 'The Prevention of Electronic Crimes Act (PECA) 2016: Understanding the Challenges in Pakistan' (2023) 2 Siazga Research Journal 273
- Keith LC, 'The United Nations International Covenant on Civil and Political Rights: Does It Make a Difference in Human Rights Behavior?' (1999) 36 Journal of Peace Research 95
- Khan AUA, 'Cyber Crime in Pakistan: Trends, Challenges, and Legal Responses: <https://doi.org/10.55966/Assaj.2025.4.1.080>' (2025) 4 ASSAJ 1358
- Klabbers J, *International Law* (Cambridge University Press 2020)
- Kosseff J, *The Twenty-Six Words That Created the Internet* (Cornell University Press 2019)
- Kuner C, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013)
- Land MK and Aronson JD, *New Technologies for Human Rights Law and Practice* (Cambridge University Press 2018)
- Lee A, 'International Human Rights Law in Digital Space: An Examination of the Need for New Legal Measures for the Protection of Rights Online'
- Little LE, 'Internet Defamation, Freedom of Expression, and the Lessons of Private International Law for the United States' (2012) 14 European Yearbook of Private International Law 2013
- Lukings M and Habibi Lashkari A, 'Comparative Legal Strategies' *Understanding cybersecurity law in data sovereignty and digital governance: An overview from a legal perspective* (Springer 2022)
- Momen MN, 'Myth and Reality of Freedom of Expression on the Internet' (2020) 43

- International Journal of Public Administration 277
- Nazir S, Asif M and Khan AUA, 'Digital Evidence in Pakistan: A Doctrinal Assessment of Admissibility and Reliability in Criminal Trials: [https://Doi.Org/10.55966/Assaj](https://doi.org/10.55966/Assaj). 2025.4. 1.0107' (2025) 4 ASSAJ 1941
- Parrish A, 'The Effects Test: Extraterritoriality's Fifth Business' (2008) 61 Vand. L. Rev. 1455
- Rocha TM, 'Digital Services Act: Towards the Digital Rule of Law' *International Conference a Digital Europe for Citizens, Data governance, Digital Markets, Digital Services* (Springer 2023)
- Ruggie JG, 'The Social Construction of the UN Guiding Principles on Business and Human Rights' *Research handbook on human rights and business* (Edward Elgar Publishing 2020)
- Ryngaert C, 'International Jurisdiction Law' *Research Handbook on Extraterritoriality in International Law* (Edward Elgar Publishing 2023)
- , 'International Jurisdiction Law' *Research Handbook on Extraterritoriality in International Law* (Edward Elgar Publishing 2023)
- Saleem HAR and others, 'Challenges Faced by the Judiciary in Implementing Cybersecurity Laws in Pakistan' (2025) 3 The Critical Review of Social Sciences Studies 1052
- Scassa T and Currie RJ, 'New First Principles- Assessing the Internet's Challenges to Jurisdiction' (2010) 42 Geo. J. Int'l L. 1017
- Shahid H, Joshi M and Kaya M, 'Cross-Border Data Flows and Conflict of Laws: A Multi-Layered Framework for Digital Trade Regulation' (2023) 2 Legal Studies in Digital Age 53
- Shaw MN, 'Does the United Nations Have a Future? If so, What May That Be?' *Reimagining the International Legal Order* (Routledge 2023)
- SHOKRI A, 'Sovereignty in Cyberspace from the Viewpoint of International Law' [2025] Asian Journal of International Law 1
- Svantesson DJB, *Solving the Internet Jurisdiction Puzzle* (Oxford University Press 2017)
- , *Solving the Internet Jurisdiction Puzzle* (Oxford University Press 2017)
- Ullah M, Haris M and Khan NU, 'Data Governance and Cross-Border Flow Regulations: A Comparative Study of China's FTAs and WTO Framework' (2025) 3 The Critical Review of Social Sciences Studies 1404
- Voigt P and Von dem Bussche A, 'The Eu General Data Protection Regulation (Gdpr)' (2017) 10 A practical guide, 1st ed., Cham: Springer International Publishing 10