The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

TRANSNATIONAL CYBERCRIMES AND THE LEGAL RESPOSIBILITIES OF INTERNET INTERMEDIARIES: CHALLENGES OF JURISDICTION, ATTRIBUTION AND ENFORCEMENT

-Mansi Varshney

ABSTRACT

The paper examines the role of internet intermediaries such as internet service providers, social media platforms, search engines, cloud service providers, and cryptocurrency exchanges in the rise of transnational cybercrime. While intermediaries enable global connectivity, they simultaneously serve as enablers of illicit activities, including online fraud, terrorism, child exploitation, ransomware, and money laundering. This paper critically analyzes the regulatory landscape across jurisdictions, focusing on international conventions such as the Budapest Convention, and national frameworks like the Indian IT Act, the U.S. CDA Section 230, and the EU's Digital Services Act. The study further explores the tension between intermediary liability, freedom of speech, privacy, and global cybersecurity. The research concludes with recommendations for harmonized international regulation to balance innovation with accountability.

Keywords: Transnational Cybercrime, Internet Intermediaries, Intermediary Liability, Jurisdictional Challenges, Internet Service Providers (ISPs)

CHAPTER - 1
INTRODUCTION

1.1 BACKGROUND OF THE PAPER

The emergence of the digital economy has transformed communication, commerce, and governance, but it has also created new avenues for criminal activities. Internet intermediaries or entities such as Internet Service Providers (ISPs), social media platforms, cloud service providers, search engines, and cryptocurrency exchanges play a central role in enabling the global exchange of data. While they facilitate access to information, innovation, and economic growth, their platforms and services have also become fertile ground for cybercriminals. Transnational cybercrime thrives because of the borderless nature of the internet. Crimes like ransomware, phishing, online child sexual exploitation, dark web trafficking, identity theft, and cross-border financial fraud rely heavily on intermediary platforms. Therefore, it increases reliance on intermediaries for communication, trade, and financial transactions. Their infrastructure provides anonymity, global reach, and often legal immunity under safe-harbor provisions.

Despite international frameworks like the Budapest Convention on Cybercrime (2001) and increasing national legislation, there remains a gap in regulating intermediaries' accountability. Balancing freedom of expression, privacy, and innovation with security imperatives poses a legal and policy dilemma. This study critically examines how internet intermediaries facilitate the expansion of transnational cybercrime and evaluates the adequacy of legal frameworks addressing their role.

1.2 LITERATURE REVIEW

1. **The OECD's 2011 publication, "The Role of Internet Intermediaries in Advancing Public Policy Objectives,"** provided a foundational analysis of the governance challenges within the digital ecosystem. The literature in this report centres on defining Internet Intermediaries (IIs) such as search engines, social media platforms, and ISPs as influential gatekeepers crucial to the flow of online information and commerce.

The report highlights the dual nature of IIs, acknowledging their immense contribution to innovation and economic growth while simultaneously grappling with the significant public policy issues they generate. The core tension discussed is how to leverage the IIs' unique

position to achieve diverse public policy objectives without stifling the internet's open nature. Key policy areas scrutinized include the effective protection of intellectual property rights, the fight against the proliferation of illegal content (such as child sexual abuse material), ensuring consumer protection and privacy, and maintaining a competitive marketplace. Fundamentally, the OECD advocates for regulatory frameworks that move beyond traditional liability models toward encouraging industry self-regulation and cooperative public-private partnerships to advance these societal goals in a technologically neutral and flexible manner.[1]

2. The Economic and Social Role of Internet Intermediaries (OECD) The existing literature consistently defines Internet intermediaries as entities that facilitate transactions or communication between third parties by providing access, hosting, transmitting, or indexing online content and services. Economically, research highlights their role as powerful enablers of growth and innovation, particularly for Small and Medium-sized Enterprises (SMEs), by lowering entry barriers, increasing price transparency, and creating new e-commerce markets, leading to significant contributions to GDP. Socially, they are viewed as crucial arbiters of public discourse, empowering users with access to information and platforms for free expression and social interaction. However, a major theme across the academic and policy landscape is the dilemma of liability and regulation. Scholars note the delicate balance required to hold intermediaries accountable for illegal or harmful content (e.g., copyright infringement, illicit trafficking) without implementing overly stringent monitoring requirements that would stifle innovation and have a chilling effect on free speech. Consequently, the focus remains on developing clear, functional legal frameworks, like "notice and take-down" regimes and conditional immunity, to address these complex policy objectives.[2]

3. Intermediary Liability in India by Pritika Rai Advani[3] this literature on intermediary liability in India offers a comprehensive analysis of legislative and judicial responses to the responsibilities of online service providers, with particular attention to the evolution and ambiguities of the governing framework. Advani delineates how Section 79 of the Information Technology Act (IT Act), established in 2000 and amended subsequently, provides the foundational safe harbour protection for intermediaries, conditional upon their

[1] OECD, *The Role of Internet Intermediaries in Advancing Public Policy Objectives* (OECD Publishing 2011) http://dx.doi.org/10.1787/9789264115644-en) accessed 26 October 2025.
[2] K Perset, 'The Economic and Social Role of Internet Intermediaries' (2010) OECD Digital Economy Papers No 171 (https://doi.org/10.1787/5kmh79zzs8vb-en) accessed 26 October 2025.
[3] Pritika Rai Advani, 'Intermediary Liability in India' (2013) **48(50)** *Economic and Political Weekly* 120.

lack of actual knowledge and diligent attempts to curb unlawful content. However, the scope and interpretation of knowledge whether actual or constructive remain contentious, contributing to persistent uncertainty regarding due diligence requirements. She discusses how the amendments to the IT Act have broadened the definition of intermediaries, shifting their role from mere conduits to entities required to actively monitor and respond to problematic third-party content. The literature highlights that such shifting expectations may undermine the neutrality and passive status of intermediaries, risking over-regulation and chilling effects on free speech. The evaluation critically notes that increasing demands on intermediaries without clear guidelines can lead to arbitrary censorship and a lack of transparency and accountability in the regulatory environment. Ultimately, she advocates for a balanced legal framework that clarifies responsibilities, preserves fundamental rights, and prevents intermediary overburdening, emphasizing transparency and proportionality in content moderation and liability.

4. The new UN Cybercrime Convention: aims and pitfalls by Metehan Durmaz

The literature on the new UN Cybercrime Convention reflects deep concern over its expansive aims and significant pitfalls. The Convention aims to enhance international cooperation in preventing and tackling cybercrime while providing a framework for the collection and exchange of electronic evidence for serious crimes across borders. However, scholars and analysts such as Metehan Durmaz highlight critical issues with the Convention's broad definitions and procedural mechanisms, warning that they risk being exploited by governments to justify intrusive surveillance, censorship, and human rights violations, particularly in countries with repressive regimes. Literature repeatedly points out the danger of the Convention's reliance on domestic laws for the definition of crimes and safeguards, which can lead to the legitimization of authoritarian practices under the guise of cybersecurity. This is compounded by vague provisions around international cooperation and mutual legal assistance, enabling states to pursue cross-border surveillance requests with little oversight or transparency. Critics contend that, despite the Convention's stated goal of combating transnational cyber threats, its flawed safeguards and overbroad scope ultimately undermine international human rights standards and threaten to facilitate the repression of free speech, dissent, and marginalized groups under the pretense of cybercrime control.[4]

[4] Metehan Durmaz, 'The New UN Cybercrime Convention: Aims and Pitfalls' (SMEX) (https://smex.org/the-new-un-cybercrime-convention-aims-and-pitfalls/) accessed 26 October 2025.

5. Talat Fatima's *Cyber Crimes* (3rd Edition, 2024)[5] It provides a comprehensive legal analysis of internet intermediaries and their pivotal role in cybercrime regulation. The book explores intermediaries as facilitators of digital communication and commerce, highlighting their dual function as enablers of innovation and potential conduits for criminal activity. Fatima critically examines the challenges in defining intermediary liability, focusing on the legal obligations under Indian and international frameworks. The work emphasizes the need for balanced regulatory approaches that safeguard user rights while ensuring effective content moderation and cooperation with law enforcement, addressing emerging threats such as cyber-enabled offenses and data privacy concerns.

1.3 STATEMENT OF PROBLEM

The proliferation of the internet and digital communication technologies has fostered an environment where transnational cybercrimes such as data breaches, financial fraud, and the dissemination of illegal content are rapidly increasing in volume, complexity, and global impact. A critical impediment to effectively combating these crimes is the complex and inconsistent legal status and responsibility of internet intermediaries (e.g., Internet Service Providers, social media platforms, cloud hosting services).

The core problem is the fundamental disharmony between the territoriality of traditional legal frameworks and the borderless nature of cyberspace, which creates significant, often insurmountable, barriers in three key areas: Jurisdiction: The difficulty in establishing which national court has the authority to hear a case when the crime, the victim, the perpetrator, and the intermediary's data or operations span multiple sovereign states, leading to jurisdictional conflicts, gaps, or overreach (the "legal arms race"). Attribution: The technological challenges of tracing anonymous cyber-attacks back to an identifiable perpetrator or source, coupled with the lack of harmonized international standards for the collection, preservation, and sharing of electronic evidence held by intermediaries in different jurisdictions. Enforcement: The practical obstacles to compelling a foreign-domiciled intermediary to comply with judicial orders (e.g., content removal or data disclosure) and the limited efficacy of international cooperation mechanisms, such as Mutual Legal Assistance Treaties (MLATs), which are often too slow to address the speed of cybercrime.This legal and operational vacuum allows cybercriminals to operate with relative impunity, undermines the security of the global digital economy, and places disproportionate or conflicting burdens on

[5] Talat Fatima, *Cyber Crimes* (3rd edn, Eastern Book Company 2021).

internet intermediaries, compelling them to become de facto regulators or law enforcement proxies without clear and universally accepted legal standards. Therefore, a comprehensive analysis of the existing legal and regulatory models is essential to propose solutions that reconcile the conflicting principles of national sovereignty, intermediary liability, and the necessity of effective transnational cybercrime prosecution.

1.4 RESEARCH OBJECTIVES

1. To examine how internet intermediaries contribute to the rise of transnational cybercrime.
2. To analyze existing international and national legal frameworks governing the regulation of intermediaries.
3. To evaluate the balance between liability, free expression, and cybersecurity.
4. To identify regulatory gaps and propose a harmonized global approach.

1.5 RESEARCH QUESTIONS

1. How do internet intermediaries contribute to the facilitation of transnational cybercrime?
2. How effective are existing legal frameworks at the international and national levels in ensuring accountability?
3. How can the regulation of internet intermediaries effectively balance intermediary liability, the protection of digital rights, and cybersecurity concerns in addressing transnational cybercrime?
4. What are the key regulatory gaps in existing legal frameworks governing internet intermediaries?
5. How can Indian legal standards governing the responsibilities of internet intermediaries be harmonized with evolving international frameworks to effectively address transnational cybercrimes

1.6 RESEARCH METHODOLOGY

The researcher adopts a doctrinal and comparative legal research design, integrating both qualitative and analytical methods. The doctrinal approach is used to examine statutory provisions, case laws, and international conventions governing the responsibilities of internet intermediaries. The comparative component analyzes differences and convergences across key jurisdictions—India, the United States, and the European Union to identify best practices and gaps in legal frameworks addressing transnational cybercrime.

1.7 HYPOTHESIS

The increasing complexity of transnational cybercrimes exposes critical gaps in the legal responsibilities of internet intermediaries, as existing jurisdictional frameworks and attribution mechanisms are insufficiently harmonized across borders, resulting in weak enforcement and inconsistent accountability standards in international cyberlaw regimes.

1.8 SCOPE AND LIMITATION

This study focuses on examining the legal frameworks, challenges, and responsibilities of internet intermediaries in the context of transnational cybercrime. It analyzes both international and domestic laws, relevant case law, and socio-legal literature to understand how intermediaries may facilitate, prevent, or mitigate such cross-border offenses. The research adopts a doctrinal methodology, relying primarily on secondary sources such as international conventions, national statutes, judicial decisions, scholarly writings, and official policy reports.

The scope is geographically confined to three key jurisdictions: India, the United States, and the European Union. These regions have been selected due to their distinct regulatory approaches and influential roles in shaping global cyber governance. However, the study acknowledges certain limitations arising from its exclusive reliance on secondary materials and the absence of primary empirical research within affected or stakeholder communities. Consequently, while the analysis provides a comprehensive legal and theoretical understanding, it does not extend to firsthand socio-technical or behavioral observations.

1.9 RATIONALE OF STUDY

The rapid expansion of digital communication and cross-border data flows has generated complex forms of cybercrime that defy territorial boundaries and challenge traditional notions of sovereignty and legal jurisdiction. Internet intermediaries, including service providers, social media companies, and digital hosting platforms, occupy a central position in this environment. They facilitate legitimate online engagement while, at times, unintentionally enabling illicit activities. Their dual role as custodians of digital infrastructure and subjects of regulatory oversight situates them within a delicate balance between protecting user rights, maintaining data privacy, and cooperating with law enforcement agencies.

However, the legal regimes governing intermediary accountability vary widely across jurisdictions. Some states enforce obligations like due diligence or content removal, whereas others prioritize immunity in support of technological development and free speech. This lack of uniformity creates jurisdictional conflicts, ambiguity in assessing liability, and considerable enforcement difficulties in cases spanning multiple nations. This research seeks to address a critical gap in international cyber law by analyzing how intermediary responsibilities can be regulated consistently and fairly across borders. It aims to advance a rights-based, harmonized framework that strengthens transnational cooperation, preserves innovation, and promotes equitable standards of accountability in combating global cyberc

CHAPTER - 2
ROLE OF INTERNET INTERMEDIARIES

2.1 INTRODUCTION

Internet intermediaries, also referred to as online service providers or digital platforms, play a central role in facilitating, enabling, and regulating digital communication, commerce, and information flow in the modern online ecosystem. Broadly, they act as conduits between end-users and digital content, providing services such as internet access, cloud hosting, social media platforms, search engines, messaging apps, and e-commerce platforms. Their primary function is to receive, store, transmit, or process data on behalf of users, often without controlling the content itself. Examples include ISPs, Facebook (Meta), Google, WhatsApp, Amazon, and cryptocurrency exchanges. Internet intermediaries occupy a dual role: they are essential enablers of digital communication, commerce, and innovation, yet they also pose regulatory and enforcement challenges, as their platforms can be misused for transnational cybercrime. In this Chapter researcher focussed on the negative role of the internet intermediaries

2.2 WHAT IS INTERMEDIARY

Definition under Indian Law

Section 2(w) of the IT Act, 2000[6] defines an intermediary as: "Intermediary means any person who on behalf of another person receives, stores or transmits any electronic record or provides any service with respect to that record."

Examples include ISPs, web hosting providers, search engines, online marketplaces, and social media platforms.

Definition under European Union Law

E-Commerce Directive 2000/31/EC (EU)[7]: "Information society service providers that provide access to a communication network, host content, or act as intermediaries in online

[6] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (India) (https://www.meity.gov.in/documents/act-and-policies/rules-for-information-technology-act/) accessed 26 October 2025.
[7] Council Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) [2000] OJ L178/1.

transactions." Updated under the Digital Services Act (DSA, 2022): Intermediaries are categorized as very large platforms, hosting services, online marketplaces, search engines, and social networks. Definition in International Context *OECD Guidelines (2011)*[8]*:* "Internet intermediaries are firms or organizations that act as conduits for online services or facilitate access to online content or services."

UNODC Cybercrime Reports: Intermediaries include ISPs, hosting providers, cloud platforms, and social media companies facilitating cross-border digital communications.

2.3 ANONYMITY AND ENCRYPTION

Internet intermediaries, while crucial for global connectivity and digital services, have inadvertently facilitated a wide range of transnational cybercrimes. Anonymity is one of the most significant features enabling cybercrime. Internet intermediaries provide services such as Virtual Private Networks (VPNs), encrypted messaging apps (e.g., Telegram, Signal), and privacy-focused browsers, which allow users to conceal their identities, locations, and online activity.

- According to Europol's Internet Organized Crime Threat Assessment (IOCTA, 2023)[9], over 60% of cross-border cybercrime operations exploit encrypted communication channels to coordinate attacks, distribute malware, or conduct fraud.
- Encrypted messaging apps have been repeatedly misused by terrorist organizations, drug trafficking networks, and child exploitation rings to communicate safely across jurisdictions.
- While encryption is vital for privacy and data security, its misuse has led law enforcement agencies to struggle with "going dark" issues, where lawful interception becomes extremely difficult.

2.4 HOSTING AND DISSEMINATION OF CONTENT

Cloud service providers, web hosting companies, and file-sharing platforms act as intermediaries by storing, transmitting, or enabling access to digital content. While most

[8] 'OECD Guidelines for Multinational Enterprises' (US Department of State Archive) (https://2009-2017.state.gov/e/eb/oecd/usncp/guidelines/index.htm) accessed 26 October 2025.
[9] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2023* (Publications Office of the European Union 2023).

content is legitimate, malicious actors exploit these services to host malware, ransomware infrastructure, extremist propaganda, and Child Sexual Abuse Material (CSAM).

- A report by UNODC (2022) indicated that over 75% of detected CSAM content was hosted on global cloud platforms, highlighting the scale of abuse[10].
- File-sharing sites are often used to distribute malware and ransomware kits; for example, the WannaCry ransomware exploited cloud-hosted command-and-control servers to propagate globally in 2017.
- Extremist groups such as ISIS have relied on social media and cloud services to disseminate propaganda, recruit members, and fundraise internationally.

2.5 GLOBAL CONNECTIVITY

Social media platforms and e-commerce intermediaries facilitate cross-border interactions, which, while socially and economically beneficial, also create avenues for fraud, scams, and money-laundering schemes.[11]

- Online marketplaces are used for illegal trade in drugs, counterfeit goods, and stolen data, which can be ordered in one country and delivered internationally.
- Social media scams such as phishing campaigns, investment fraud, and romance scam have a global footprint, affecting millions of users annually. According to Interpol (2023), cross-border online fraud increased by 35% between 2020 and 2022, often exploiting social media platforms as intermediaries[12].
- The global reach of intermediaries complicates detection, as perpetrators operate from jurisdictions with weak cybercrime laws or minimal enforcement capacity.

2.6 FINANCIAL INTERMEDIARIES: CRYPTOCURRENCY EXCHANGES

Cryptocurrency exchanges, digital wallets, and online payment intermediaries play a dual role: they facilitate legitimate transactions while enabling cybercriminal financial operations.

[10] UNODC, *Global Report on Trafficking in Persons 2022* (https://www.techuk.org/resource/report-unodc-global-report-on-trafficking-in-persons-2022.html) accessed 26 October 2025.
[11] Andrew Daly, 'The Invisible Intermediaries Delivering a Seamless Online Experience' (Analysys Mason) (https://www.analysysmason.com/consulting/articles/seamless-online-experience/) accessed 26 October 2025.
[12] Europol European Cybercrime Centre (EC3), *Internet Organised Crime Threat Assessment (IOCTA) 2023* (9th edn, Issue 2, 2023) 145–46.

- Ransomware attacks now routinely demand cryptocurrency payments, which can be routed through intermediaries across multiple countries to obscure the trail.
- According to Chainalysis 2024 saw a value received by illicit cryptocurrency addresses to a total of $40.9 billion. For instance, when we published last year's Crypto Crime Report, we reported $24.2 billion for 2023. ,with ransomware, darknet markets, and fraud being the largest contributors.[13]
- Lack of uniform regulation across exchanges and jurisdictions allows criminals to launder funds quickly, making prosecution and asset recovery challenging.

2.7 CASE STUDIES

1. ISIS Online Propaganda:

The best-known legal case focused specifically on ISIS online propaganda is *Twitter, Inc. v. Taamneh*[14], decided by the United States Supreme Court in May 2023. This case addressed allegations that major social media platforms like Twitter, Facebook, and Google provided material assistance to ISIS by allowing and algorithmically promoting the group's propaganda and recruitment material online. The Court ultimately found that the platforms could not be held liable for merely hosting and recommending such content, ruling that their actions were not equivalent to providing substantial assistance to ISIS. ISIS used Telegram, Twitter, and cloud-hosted sites to recruit members and coordinate operations globally. Law enforcement struggled due to encryption and cross-border hosting.

2. Silk Road Dark Web Marketplace:

Silk Road facilitated anonymous trade in drugs and illicit goods, relying on Tor networks and cryptocurrency intermediaries to evade detection. *"United States v. Ross Ulbricht*."[15]. This federal criminal case was tried in the Southern District of New York and centered on Ross William Ulbricht, the creator and operator of the Silk Road marketplace, who was convicted

[13] Chainalysis, *2025 Crypto Crime Report: Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized* (15 January 2025).
[14] *Twitter, Inc. v. Taamneh* 598 U.S. 471 (2023).
[15] *United States v. Ross Ulbricht* 858 F.3d 71 (2d Cir. 2017)

on multiple charges including drug trafficking, money laundering, and conspiracy related to the operation of the darknet site.[16]

3. Ransomware Crypto Payments: *G&G Oil Co. of Indiana v. Continental Western Insurance Co. (Ind. 2021)*[17] The Indiana Supreme Court addressed insurance coverage for a ransomware bitcoin payment, setting an important precedent in interpreting insurance policies as they relate to ransomware crypto payments.

4. Cambridge Analytica Scandal:

Misuse of Facebook as an intermediary for harvesting personal data for political campaigns showed how intermediaries can be exploited without breaking traditional laws. This case involved the misuse of Facebook user data by the political consulting firm Cambridge Analytica and resulted in investigations, regulatory actions, and various court and ADMINISTRATIVE CASES ACROSS THE US, UK, AND OTHER COUNTRIES

2.9 CONCLUSION

The examination of internet intermediaries within the context of transnational cybercrime reveals their complex and often contradictory position in the global digital ecosystem. These entities ranging from ISPs and social media companies to cloud providers and cryptocurrency exchanges serve as essential enablers of communication, commerce, and innovation. Yet, their technological capabilities and vast reach have also created new avenues for criminal activity that transcend territorial boundaries and challenge traditional law enforcement mechanisms.

Anonymity, encryption, and global connectivity, while vital for privacy and digital freedom, simultaneously facilitate cyber-enabled crimes such as ransomware attacks, illicit trade, online fraud, and extremist propaganda. The studied cases, including Twitter v. Taamneh, United States v. Ross Ulbricht, and the Cambridge Analytica investigations, highlight how intermediaries may be misused to advance illegal acts or undermine regulatory safeguards. Moreover, the lack of uniform regulation, coupled with jurisdictional fragmentation and

[16] FBI, 'Ross Ulbricht, the Creator and Owner of the Silk Road Website, Found Guilty in Manhattan Federal Court on All Counts' (Press Release, 4 February 2015 (https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/ross-ulbricht-the-creator-and-owner-of-the-silk-road-website-found-guilty-in-manhattan-federal-court-on-all-counts) accessed 26 October 2025.

[17] Ransomware Crypto Payments: *G&G Oil Co. of Indiana v. Continental Western Insurance Co. (Ind. 2021)*165 N.E.3d 82 (Ind. 2021).

inconsistent enforcement, has allowed cybercriminals to exploit legal loopholes and evade accountability.

This chapter underscores the urgent need for a harmonized international framework that defines intermediary liability, strengthens cross-border cooperation, and ensures both accountability and human rights protection. Effective governance of intermediaries must strike a balance between fostering digital innovation and safeguarding global cybersecurity, transparency, and the rule of law.

CHAPTER – 3
INTERNATIONAL LEGAL FRAMEWORK GOVERNING INTERMEDIARIES

3.1 INTRODUCTION

This Chapter examines the evolution and contemporary relevance of international instruments addressing cybercrime, focusing primarily on the Budapest Convention on Cybercrime (2001), the ongoing United Nations Cybercrime Treaty (2024), and complementary mechanisms such as Interpol, Europol, and Mutual Legal Assistance Treaties (MLATs). The discussion begins with an assessment of the Budapest Convention's landmark role as the first binding international treaty dedicated to combating cybercrime, analyzing its strengths such as harmonized legal standards, robust cooperation mechanisms, and human rights safeguards and its limitations, particularly regarding participation gaps and outdated data protection norms.

Further, the chapter delves into the operational dimensions of international cooperation, evaluating the role of Interpol, Europol, and MLATs in facilitating cross-border investigations and digital evidence exchange. Finally, it addresses the challenges of international collaboration in regulating intermediaries, including jurisdictional conflicts, divergent liability regimes, political tensions, and disparities in enforcement capacity.

3.2 BUDAPEST CONVENTION ON CYBERCRIME (2001)

The Budapest Convention on Cybercrime (2001), also known as the Council of Europe Convention on Cybercrime (CETS No. 185), is widely recognized as the first and most significant binding international treaty dedicated to addressing crimes committed via the internet and other computer networks. Opened for signature in Budapest in November 2001, and entering into force in 2004, it aimed to harmonize national laws, improve investigative techniques, and enhance international cooperation. The Convention establishes a comprehensive legal framework for states to criminalize certain activities such as illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related fraud, child pornography, and copyright violations.[18]

3.2.1 Strengths

[18] Convention on Cybercrime (adopted 23 November 2001, entered into force 1 July 2004) ETS 185 (Budapest Convention) (https://www.coe.int/en/web/cybercrime/the-budapest-convention) accessed 26 October 2025.

The Budapest Convention's greatest achievements are derived from its role as a global legislative template and its success in institutionalizing cross-border law enforcement cooperation.

The Budapest Convention (BC) holds a unique status as the first international treaty on cybercrime, functioning as a global benchmark and model law for domestic legislation, even among non-CoE members. Its influence is reflected in its widespread adoption by 78 Parties and its continued relevance amid emerging competing frameworks. A major strength of the Convention lies in its robust international cooperation framework, which mandates extensive collaboration among member states through provisions for Mutual Legal Assistance (MLA), expedited data preservation, and access to subscriber information. Operationally, the Convention's 24/7 Network plays a pivotal role in facilitating rapid, real-time support for cross-border investigations and ensuring the admissibility of electronic evidence. The Second Additional Protocol (2022) further strengthens this operational structure by expanding cooperation, particularly with private sector entities. Moreover, the Convention exerts significant institutional influence over global technology companies, especially in data disclosure practices. Service providers commonly recognize the BC as a trusted legal framework, with compliance rates reaching about two-thirds of data requests from parties. Rooted in its strong procedural safeguards and commitment to human rights under Article 15, the Convention has successfully bridged the gap between national jurisdictions and the global data control exercised by private intermediaries.[19]

3.2.2 LIMITATIONS

The effectiveness of the Budapest Convention on Cybercrime is constrained by a lack of universal participation, with major powers such as Russia, China, India, and Brazil refusing to accede due to concerns over sovereignty and data control. This fragmentation has deepened following the adoption of the 2024 UN Convention Against Cybercrime, which reflects competing geopolitical interests and differing approaches to state authority and human rights. Moreover, the Budapest Convention's outdated data protection framework, rooted in pre-GDPR standards and reliant on Convention 108, creates regulatory friction in

[19] *Convention on Cybercrime* (adopted 23 November 2001, entered into force 1 July 2004) ETS 185

cross-border data transfers. Together, these factors undermine global harmonization, hinder cooperation, and complicate enforcement in addressing transnational cybercrime.[20]

3.3 ONGOING UN TREATY ON CYBERCRIME NEGOTIATIONS.

The Budapest Convention's limitations and expanding global cybercrime landscape led the UN to draft a new Comprehensive International Convention on Countering the Use of ICTs for Criminal Purposes, initiated by an Ad Hoc Committee in 2019 to achieve universal consensus. Unlike the Eurocentric Budapest Convention, the UN treaty includes all member states, including major holdouts like Russia, China, and India, aiming to cover both cyber-dependent and cyber-enabled crimes comprehensively. Its goals are to harmonize substantive and procedural cybercrime laws and improve international cooperation through extradition, mutual legal assistance, and real-time data sharing. A major focus is clarifying internet intermediaries' responsibilities to prevent misuse for terrorism, fraud, and exploitation, while also preserving safe harbour principles to protect innovation and expression.[21]

However, negotiations face significant controversies: Western states prefer a narrow focus on cyber-dependent crimes, whereas others push to include hate speech and disinformation, raising censorship concerns. Debates also centre on cross-border data access, with some states promoting streamlined mechanisms and others defending sovereignty and privacy rights. Civil society warns against vague definitions and expansive surveillance powers threatening human rights. The treaty remains in draft as of 2025, with geopolitical divides between the Western Bloc and other states stalling progress. Its success depends on balancing sovereignty, security, human rights, and private sector accountability, aiming for the first truly universal, rights-respecting global cybercrime framework. This treaty was adopted by the UN General Assembly in December 2024, with 65 nations signing by October 2025 and it awaits further ratifications to enter into force.[22]

3.4 RELATED TO EU AND INDIA

The United Nations General Assembly established an Ad Hoc Committee in 2019 to draft a Comprehensive International Convention on Countering the Use of ICTs for Criminal Purposes, known as the UN Cybercrime Treaty. This treaty aims to create a globally inclusive

[20] UNODC, 'United Nations Convention against Cybercrime' https://www.unodc.org/unodc/en/cybercrime/convention/home.html accessed 20 October 2025.
[21] Vibhu Mishra, 'Sixty-Five Nations Sign First UN Treaty to Fight Cybercrime, in Milestone for Digital Cooperation' (UN News, 25 October 2025).
[22] UNGA, 'Draft United Nations Convention Against Cybercrime' (7 August 2024) UN Doc A/AC.291/L.15..

framework that addresses traditional and cyber-enabled crimes, overcoming the limitations of the Budapest Convention's Eurocentric focus and restricted membership. The EU supports the treaty cautiously, prioritizing harmony with existing laws like the GDPR and ECHR, emphasizing human rights safeguards and judicial oversight, while expressing concerns about potential misuse by states to expand surveillance or suppress dissent. India, having not ratified the Budapest Convention, seeks a broader treaty scope that includes cyber-enabled crimes and emphasizes capacity building for developing countries. It supports strong cooperation measures but remains cautious about embedding strict human rights language, balancing sovereignty and national security concerns. These contrasting positions reflect a broader North-South divide, with the EU advocating a rights-centric, narrowly focused treaty, and India advocating for a comprehensive, state-centric approach addressing diverse cybercriminality and sovereignty. The negotiation tensions revolve around offense definitions, intermediary liability, and data-sharing safeguards, illustrating the challenges in crafting a universally accepted cybercrime governance framework.[23]

3.5 ROLE OF INTERPOL, EUROPOL, AND MLATS IN CROSS-BORDER ENFORCEMENT.

International cooperation is essential to combat the cross-border nature of cybercrime, as no single country can tackle offenses spanning multiple jurisdictions alone. Interpol acts as a global platform for intelligence sharing and coordination through initiatives like its Cyber Fusion Centre and joint operations, though it relies on member states' voluntary cooperation. Europol, the EU's law enforcement agency, offers a more integrated regional model with the European Cybercrime Centre (EC3), facilitating joint investigations and forensic support under harmonized EU legal standards. Mutual Legal Assistance Treaties (MLATs) provide the formal legal framework enabling states to request digital evidence and investigative support from each other, but these mechanisms are often slow, bureaucratic, and subject to diplomatic challenges. Together, these institutions form a multilayered cooperation system crucial for effective cybercrime enforcement, yet face challenges like jurisdictional fragmentation, delayed responses, and rapidly evolving cyber threats. This underscores the

[23] Pradeep Kulshreshtha and others (eds), *Cyber Crime, Regulations and Security* (1st edn, 2023) 90.

urgent need for streamlined, technology-adaptive enforcement mechanisms to enhance intermediary regulation and cross-border collaboration. [24]

3.6 Challenges of international cooperation in regulating intermediaries.

The fight against transnational cybercrime faces significant challenges in international cooperation, primarily due to the internet's borderless nature allowing perpetrators, victims, and intermediaries to span multiple jurisdictions. Jurisdictional conflicts arise as national laws differ, such as the EU's stringent Digital Services Act versus the US's more permissive Section 230 safe harbor, complicating enforcement. Legal and definitional inconsistencies concerning cybercrime and intermediary responsibility create loopholes that criminals exploit. Political and sovereignty issues further hinder cooperation, especially with authoritarian states wary of external interference. Technical and procedural barriers, including slow Mutual Legal Assistance Treaties (MLATs), encryption, and intermediaries' reluctance to share data, obstruct investigations. Finally, disparities in capacity between developed and developing nations allow cyber offenders to exploit weaker jurisdictions with limited enforcement, undermining global efforts. Addressing these challenges requires harmonized legal frameworks, enhanced technical capacity building, and stronger, faster multilateral collaboration to effectively regulate intermediaries and combat cybercrime worldwide.[25]

3.7 Conclusion

The Budapest Convention on Cybercrime (2001) stands as the first comprehensive international treaty addressing internet-related crimes, aiming to harmonize national laws, enhance investigative methods, and facilitate international cooperation. It criminalizes offenses such as illegal access, data interference, interception, misuse of devices, computer-related fraud, and child pornography. A key strength lies in its robust framework for cross-border law enforcement cooperation, including Mutual Legal Assistance, expedited data preservation, and the establishment of a 24/7 network for rapid response. Its procedural safeguards uphold human rights by aligning with international human rights laws. However, limitations stem from non-universal adoption, especially by major powers like Russia, China, India, and Brazil due to sovereignty concerns. Additionally, its data protection standards lag

[24] Elena Vlădulescu, 'The Cooperation between Europol and Interpol in the Field of Combating Cross Border Crimes' (2012) 2(3) International Journal of Criminal Investigation 171.
[25] Arum Widiastuti and Yasmirah Mandasari Saragih, 'Transnational Cyber Crime: Challenges of International Cooperation in Combating Cybercrime' (2025) 2(9) International Journal of Contemporary Sciences 1004.

behind modern frameworks like the GDPR, causing cross-border data sharing complexities. The ongoing UN Cybercrime Treaty initiated in 2019 seeks a universal, inclusive framework addressing these gaps, but geopolitical divides and differing priorities among states pose challenges. Institutions like Interpol, Europol, and MLATs play vital but sometimes limited roles in enforcement, facing bureaucratic and jurisdictional hurdles. The chapter underscores the critical need for adaptive, rights-respecting, and technologically adept legal regimes to enhance intermediary regulation and strengthen international cooperation against transnational cybercrime

CHAPTER – 4
NATIONAL LEGAL APPROACHES TO INTERMEDIARY LIABILITY

4.1 INTRODUCTION

As the digital ecosystem expands globally, the regulation of internet intermediaries has become central to balancing innovation, accountability, and fundamental rights. Different jurisdictions have developed distinct legal frameworks to determine when intermediaries such as social media platforms, internet service providers, and search engines should be held responsible for user-generated content. This chapter provides a comparative analysis of intermediary liability regimes in the United States**,** European Union, and India, highlighting how each reflects its underlying legal culture and policy priorities. The U.S. model, rooted in Section 230 of the Communications Decency Act, favours broad immunity to protect free expression and innovation. The EU, through the Digital Services Act (DSA) and the General Data Protection Regulation (GDPR), adopts a rights-based and accountability-focused approach emphasizing transparency and user protection. India, under the Information Technology Act and Intermediary Guidelines Rules, follows a more state-centric and security-driven model, placing stricter compliance obligations on intermediaries.

4.2 UNITED STATES

The United States has historically adopted one of the most permissive approaches to intermediary liability. The cornerstone of this framework is Section 230 of the Communications Decency Act (CDA) of 1996, which broadly immunizes internet intermediaries from liability for content posted by third parties. Section 230 states that providers of "interactive computer services" shall not be treated as publishers of information provided by users, thereby shielding platforms like social media companies, ISPs, and online forums from lawsuits over user-generated content. This safe-harbor provision has been credited with enabling the growth of major U.S. technology companies, fostering innovation and free expression online.[26]

However, Section 230 has also been subject to intense criticism. Critics argue that it grants overly broad immunity, allowing intermediaries to avoid accountability for hosting harmful

[26] Saman Devgan, 'Cybercrime and Social Media Platforms: Legal Accountability in the Indian Context' (2024) 4(2) International Journal of Law, Justice and Jurisprudence 326.

content such as hate speech, disinformation, or child sexual abuse material (CSAM). In recent years, bipartisan calls for reform have grown stronger. Proposals include narrowing immunity, requiring greater content moderation obligations, or introducing carve-outs for harmful categories of speech. The U.S. Supreme Court cases of *Gonzalez v. Google* (2023)[27] and *Twitter v. Taamneh*[28] have highlighted tensions around whether algorithms that recommend harmful content fall under Section 230 protections. Reform debates remain unresolved, reflecting the difficulty of balancing free speech protections under the First Amendment with the need for platform accountability.

4.3 EUROPEAN UNION

The European Union has evolved from the E-Commerce Directive of 2000, which introduced a conditional safe harbor for intermediaries, to the more comprehensive Digital Services Act (DSA) of 2022**.** Under the E-Commerce Directive, intermediaries were not liable for illegal content provided they acted as passive conduits and removed such content upon receiving notice ("notice-and-takedown" regime). While groundbreaking at the time, this framework became outdated as online platforms grew into powerful gatekeepers[29].

The Digital Services Act (DSA) represents a paradigm shift by imposing proactive obligations on intermediaries, especially "very large online platforms" (VLOPs) such as Facebook, Twitter (X), and YouTube. The DSA requires risk assessments, transparency reports, mandatory cooperation with regulators, and stronger mechanisms for user redress. It also introduces obligations to address systemic risks such as disinformation, election interference, and harmful algorithmic amplification. Complementing this is the General Data Protection Regulation (GDPR, 2018)**,** which imposes stringent requirements on intermediaries handling personal data, including user consent, data minimization, and penalties for breaches. Together, the DSA and GDPR reflect the EU's rights-centered approach, aiming to balance liability with digital rights and data protection.

4.4 INDIA

[27] *Gonzalez v. Google* 598 U.S. 617 (2023)
[28] *Twitter, Inc. v. Taamneh* 598 U.S. 471 (2023).
[29] European Commission, 'The Digital Services (https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en) accessed 26 October 2025.

India's approach is primarily governed by the Information Technology Act, 2000, and its subsequent amendments. Section 79 of the IT Act initially provided safe harbor protections to intermediaries, exempting them from liability for third-party content if they acted as mere conduits and complied with lawful directions. However, over time, the Indian government has introduced stricter obligations on intermediaries. *Kunal Kamra v. Union of India* (2024)[30]: The court held intermediaries lose "safe harbour" only if they fail to comply with due diligence under Section 79, and that ultimate decisions on unlawful content rest with courts, not government agencies or fact-check units. The Court struck down sub-clause (v) of Rule 3(1) (b)[31] of the the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**.**

The most significant shift came with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. The 2022 amended Rule 3(1)(b) of the Information Technology Act (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, requires intermediaries to exercise "reasonable efforts by itself" to prevent users from hosting or sharing prohibited content. These rules mandate due diligence requirements, including appointment of compliance officers, grievance redressal mechanisms, and proactive content takedown obligations. Social media platforms with more than five million users must also enable traceability of messages, a requirement that raises concerns about weakening end-to-end encryption and violating user privacy. Moreover, intermediaries risk losing their safe harbor immunity if they fail to comply with these rules. This creates a more state-centric model, giving authorities significant control over online content and raising debates about censorship and freedom of expression.[32]

In National Legal Approaches to Intermediary Liability, Section 79 of the Information Technology Act, 2000 was interpreted to clarify the circumstances in which intermediaries could be held liable for online content. The Court determined that intermediaries can only remove online content if they are compelled to do so by an adjudicatory body issuing an order. Online intermediaries can avoid being held liable if they promptly remove the alleged

[30] *Kunal Kamra v. Union of India* SCC OnLine Bom 3025 (2024)
[31] Yohann Titus Mathe, 'Rule 3(1)(b), Intermediary Liability, and the Burden of "Reasonable Efforts"', (Indian Journal of Law and Technology)
[32] Daniel Seng and Ignacio Garrote Frenandez-Diez, 'Comparative Analysis of National Approaches of the Liability of the Internet Intermediaries' (WIPO) 26 (https://www.wipo.int/en/web/copyright/internet-intermediaries) accessed 26 October 2025.

illegal material from their website within a specified time frame after receiving an order from the appropriate government.[33]

4.5 COMPARATIVE INSIGHTS: BALANCING LIABILITY, INNOVATION, AND RIGHTS.

The U.S., EU, and Indian approaches to intermediary liability demonstrate divergent regulatory philosophies shaped by constitutional principles, political priorities, and societal values. The U.S. model prioritizes free expression and innovation, often at the expense of accountability. The EU model emphasizes user rights, data protection, and systemic accountability**,** while still fostering innovation within a heavily regulated framework. India's approach, by contrast, reflects a security- and sovereignty-driven model, imposing greater obligations on intermediaries to comply with government directives, sometimes at the expense of digital rights.

A comparative analysis reveals a common challenge: finding the right balance between intermediary immunity, content moderation responsibilities, innovation, and protection of fundamental rights. Excessive liability risks stifling technological innovation and free speech, while overly broad immunity allows harmful content to proliferate unchecked. The diversity in national approaches also poses problems for cross-border enforcement, as global intermediaries must navigate conflicting obligations. This reinforces the need for a harmonized international framework that sets minimum global standards for intermediary liability, while allowing flexibility for states to address local concerns.

4.6 CONCLUSION

The United States' approach to intermediary liability, anchored by Section 230 of the Communications Decency Act, exemplifies a permissive legal framework that has fueled internet innovation and free expression by broadly immunizing intermediaries from liability for user-generated content. However, this broad immunity has also raised serious concerns about accountability, particularly in relation to harmful content such as hate speech, disinformation, and child sexual abuse material. Recent legal challenges like Gonzalez v. Google (2023) and Twitter v. Taamneh have intensified scrutiny over the scope of Section

[33] Abhinav Gupta, 'The Liabilities of Internet Intermediaries for Cybercrimes' (2023) 1(1) *[Alliance Journal of Corporate and Commercial Law]* E-ISSN 2584-2463.

230 protections, especially regarding algorithmic content recommendations. The ongoing debate reflects the complex challenge of reconciling the cherished value of free speech under the First Amendment with the growing demand for more responsible platform governance. This chapter underscores that reforming intermediary liability in the U.S. context remains a delicate balancing act, with potential implications for global cyber governance and regulatory norms.

CHAPTER- 5
CRITICAL ANALYSIS AND EMERGING ISSUES

5.1 INTRODUCTION

The regulation of internet intermediaries lies at the heart of modern digital governance, balancing innovation, accountability, and fundamental rights. As online platforms increasingly shape communication, commerce, and information exchange, questions of liability, free expression, and cybersecurity have become central to international and domestic policy debates. This chapter critically examines the evolving frameworks governing intermediary responsibility, beginning with the limitations of safe-harbor regimes that grant broad immunity while failing to address today's complex digital risks. It explores the conflicts between liability, freedom of expression, and cybersecurity, the tension between corporate responsibility and state regulation, and the emerging challenges posed by AI, algorithmic harms, and cross-border enforcement. The chapter also discusses the growing role of private companies as quasi-law enforcement actors, highlighting the need for transparent, rights-based oversight. Together, these themes underscore the urgent necessity of a balanced, adaptive, and human rights oriented approach to intermediary regulation in the digital era.

5.2 LIMITATIONS OF SAFE-HARBOR REGIMES

Safe-harbor frameworks, while designed to protect innovation and shield intermediaries from undue liability, often fall short in addressing the complexities of today's digital ecosystem. One major limitation is their one-size-fits-all application, which fails to account for the vastly different roles of intermediaries from small web hosts to multinational social media platforms with billions of users. Safe harbors may unintentionally create perverse incentives, where platforms underinvest in content moderation due to broad immunity. Furthermore, the notice and takedown approach has been criticized for being reactive and ineffective against rapidly proliferating illegal content, such as extremist propaganda or CSAM, which can resurface across platforms almost instantly.[34] Overly broad immunity also leaves victims of online harms without effective remedies, undermining public trust in digital governance.

[34] Jason H Peterson, Lydia Segal and Anthony Eonas, 'Global Cyber Intermediary Liability: A Legal & Cultural Strategy' (2014) 34 Pace L Rev 586, 597.

5.3 CONFLICT BETWEEN LIABILITY, FREE EXPRESSION, AND CYBERSECURITY

The regulation of intermediaries reveals a fundamental tension between three competing values: liability, free expression, and cybersecurity. On one hand, imposing strict liability on intermediaries could incentivize more robust content moderation, but it risks chilling free speech and undermining democratic discourse, especially in countries where governments may exploit liability rules to censor dissent. On the other hand, granting broad immunity encourages free expression and innovation, but leaves significant gaps in cybersecurity protections, as platforms may fail to proactively address threats like ransomware, misinformation, or cyber fraud. Striking this balance is particularly challenging in jurisdictions like India, where safe-harbor immunity is contingent on compliance with government takedown orders, raising concerns about state overreach. The conflict highlights the difficulty of designing a liability regime that simultaneously safeguards civil liberties and strengthens resilience against cybercrime.[35]

5.4 CORPORATE RESPONSIBILITY VS. STATE REGULATION

The debate over intermediary liability also reflects a broader struggle between corporate responsibility and state regulation. Large technology companies such as Meta, Google, and Twitter wield immense power over online discourse, often shaping global standards for content moderation and data governance. While some argue that corporations should exercise greater responsibility as global digital stewards, critics highlight the risks of leaving public-interest decisions to private entities driven by profit motives. State regulation provides a democratic mechanism of accountability, but risks politicization, censorship, and jurisdictional overreach. The tension is evident in the U.S., where platforms resist government intervention under the First Amendment, and in the EU, where regulatory instruments like the DSA aim to formalize corporate responsibility under legal oversight. The challenge lies in crafting a hybrid model that ensures corporate accountability while safeguarding fundamental rights and preventing state abuse of power.

5.5 EMERGING CHALLENGES

[35] OECD, *The Role of Internet Intermediaries in Advancing Public Policy Objectives* (OECD Publishing 2011) (http://dx.doi.org/10.1787/9789264115644-en) accessed 26 October 2025.

The rapidly evolving digital landscape presents new challenges that existing safe-harbor and liability frameworks were never designed to address. These include:

- Algorithmic amplification of harmful content, where recommendation systems boost disinformation or extremist narratives.[36]
- Artificial Intelligence (AI) and Deepfakes, which make detection of false or harmful content increasingly difficult.
- Cross-border data flows, where jurisdictional conflicts complicate enforcement against global intermediaries.
- Encryption and privacy concerns, particularly with "traceability" requirements in India that may weaken security while attempting to ensure accountability.
- Cyber-enabled financial crimes, with cryptocurrencies enabling anonymous transactions for ransomware, money laundering, and dark-web marketplaces.

These challenges demand more adaptive, technology-neutral legal frameworks that can evolve alongside emerging threats while protecting user rights.

5.6 THE ROLE OF PRIVATE COMPANIES AS "QUASI-LAW ENFORCEMENT" ACTORS

A particularly contentious issue is the growing role of private technology companies as "quasi-law enforcement" actors. Platforms are increasingly expected to detect, investigate, and remove illegal content, cooperate with law enforcement agencies, and even suspend accounts linked to criminal or extremist activity. For example, tech companies routinely share data under Mutual Legal Assistance Treaties (MLATs) or emergency disclosure requests, and some actively use AI to scan for CSAM or terrorist propaganda.

While this trend enhances the fight against cybercrime, it raises serious concerns. First, delegating policing powers to private companies blurs the line between public authority and corporate governance, undermining due process and accountability. Second, enforcement is often opaque, with limited transparency about takedown algorithms, moderation decisions, or error rates. Third, global intermediaries face conflicting obligations, as compliance with one

[36] Kinga Sorbán, 'The Role of Internet Intermediaries in Combatting Cybercrime: Organisation and Liabilities' (2019) 335 Central and Eastern European EDem and EGov Days.

country's laws (e.g., government surveillance in authoritarian regimes) may violate international human rights standards. Ultimately, while private companies play an indispensable role in digital policing, their expanding quasi-law enforcement function must be tempered with oversight, transparency, and democratic accountability to prevent abuses of power.[37]

5.7 CONCLUSION

This chapter critically examines the multifaceted challenges and emerging issues in regulating internet intermediaries within the context of transnational cybercrime. Safe-harbor regimes, while safeguarding innovation and free expression, suffer from broad immunities that can undermine effective content moderation and victim redress. The enduring tension between intermediary liability, freedom of speech, and cybersecurity demands a delicate balance, especially in jurisdictions with divergent legal and political landscapes. Furthermore, the debate between corporate responsibility and state regulation highlights the need for a hybrid accountability model that protects fundamental rights while preventing governmental overreach or unchecked private power. Emerging technological threats such as algorithmic amplification, AI-generated deepfakes, and encrypted financial crimes exacerbate existing regulatory gaps and necessitate adaptable, technology-neutral legal frameworks. A significant concern is the rise of private companies as quasi-law enforcement actors, which, despite enhancing cybercrime responses, raises transparency, due process, and human rights challenges. Ultimately, effective governance requires transparent oversight mechanisms, international cooperation, and a rights-respecting approach that aligns corporate actions with democratic accountability.

[37] Giovanni De Gregorio and Roxana Radu, 'Digital Constitutionalism in the New Era of Internet Governance' (2022) 30(1) International Journal of Law and Information Technology 68.

CHAPTER – 6
CONCLUSION

6.1 INTRODUCTION

The rapid expansion of digital platforms has made internet intermediaries central to both enabling connectivity and combating cybercrime. However, existing legal regimes governing intermediary liability remain fragmented, inconsistent, and often outdated. Divergent approaches across jurisdictions ranging from the U.S. safe-harbor model to the EU's rights-based framework and India's conditional liability system have created regulatory gaps that undermine global cybersecurity and complicate cross-border enforcement.

This chapter examines the regulatory inconsistencies in current frameworks, emphasizing the urgent need for harmonization to ensure coherence, accountability, and protection of fundamental rights. It further proposes a model framework for balancing intermediary accountability with freedom of expression, privacy, and innovation through a multi-stakeholder, rights-based approach. By advancing toward harmonized global standards, the chapter underscores the importance of predictable, equitable, and adaptive governance in addressing the evolving challenges of the digital age.

6.2 CONCLUSION

The findings of this research affirm the hypothesis that the increasing complexity of transnational cybercrimes exposes significant deficiencies in the legal responsibilities and accountability mechanisms governing internet intermediaries. The comparative analysis of India, the United States, and the European Union reveals that while each jurisdiction has instituted distinct laws to regulate intermediary conduct, these frameworks remain fragmented and lack cross-border coherence. This divergence has produced inconsistent liability standards, jurisdictional overlaps, and enforcement challenges that undermine the global effectiveness of cybercrime prevention and prosecution.

Current attribution and jurisdictional models are often unable to address the territorial ambiguities inherent in digital networks, leaving enforcement agencies constrained by conflicting laws and limited international cooperation. The study thus concludes that the absence of harmonized norms and mutual legal assistance mechanisms continues to weaken accountability and hinder timely responses to cyber offenses involving multiple jurisdictions.

To move toward stronger governance, states must foster transnational cooperation through updated treaties, shared standards for intermediary responsibility, and the integration of human rights safeguards. Building a coherent and balanced international framework is essential to ensuring that innovation, privacy, and security coexist within a more accountable global cyberspace.

6.3 NEED FOR HARMONIZATION OF LAWS ON INTERMEDIARY LIABILITY

Given the global nature of cybercrime, a fragmented approach to intermediary liability is unsustainable. Harmonization of laws is essential to ensure predictability, consistency, and fairness in how intermediaries are regulated across jurisdictions. Without harmonization, intermediaries face conflicting obligations: a platform complying with the EU's stringent requirements may simultaneously breach U.S. free speech protections or India's traceability rules. Harmonization would reduce these conflicts by establishing minimum global standards on intermediary liability, striking a balance between state sovereignty and international cooperation. Moreover, harmonized laws would strengthen cross-border investigations, making it easier for law enforcement to access evidence and ensure accountability. At the same time, harmonization must recognize cultural and political differences, embedding flexible safeguards for free expression, privacy, and due process to avoid becoming a tool for censorship or state overreach. The growing momentum behind the UN Cybercrime Treaty negotiations underscores the urgency of moving toward such a coordinated approach.[38]

6.4 PROPOSED MODEL FRAMEWORK

A harmonized global framework must adopt a multi-stakeholder, rights-based model that balances accountability, fundamental freedoms, and technological innovation. Such a framework should rest on three key pillars:

1. Clear Obligations of Due Diligence – Intermediaries should be required to exercise proportionate due diligence in monitoring and responding to unlawful activities, with differentiated standards depending on their size, role, and market power. For example, social media giants could be subject to stricter proactive monitoring obligations, while smaller startups may only be expected to comply with notice-based takedown mechanisms.

[38] Pritika Rai Advani, 'Intermediary Liability in India' (2013) 48(50) Economic and Political Weekly (JSTOR) 120.

2. Safeguards for Rights and Freedoms – Any liability regime must incorporate strong procedural safeguards to protect free expression and privacy. This includes transparency in content moderation decisions, independent appeals mechanisms, and protection against arbitrary government censorship. Encryption and privacy-preserving technologies should not be weakened under the guise of accountability but rather integrated with lawful and rights-respecting access frameworks.[39]

3. Innovation-Friendly Flexibility – The model should avoid rigid one-size-fits-all rules that stifle technological progress. Instead, it should promote technology-neutral standards, regular review mechanisms to adapt to emerging threats (e.g., AI-driven cybercrime), and encourage public-private partnerships for information-sharing and best practices.

6.5 SUGGESTIONS

Enhanced due diligence obligations

- Strengthen requirements for intermediaries to proactively review, moderate, and respond to unlawful content with clear deadlines (such as the 36-hour rule under the IT Act).
- Mandate regular, transparent assessments of policies and technical systems to ensure compliance with human rights and due diligence standards.
- Require intermediaries to maintain robust cybersecurity infrastructure and rapid reporting mechanisms for security breaches and suspicious activities.[40]

Transparency and reporting standards.

- Intermediaries should publicly disclose moderation policies, content removal processes, and explanations for flagged or deleted material in alignment with fairness and due process.
- Annual transparency reports detailing actions taken against illegal content should be made easily accessible and machine-readable for accountability purposes.[41]

[39] Global Network Initiative, 'GNI 2025 Annual Learning Forum: Navigating Global Paradigm Shifts to Protect Digital (https://globalnetworkinitiative.org/gni-2025-annual-learning-forum-navigating-global-paradigm-shifts-to-protect-digital-rights/) accessed 26 October 2025.
[40] Manisha Debnath, 'Intermediary Liability in the Digital Age: Balancing Corporate Responsibility and Cybersecurity' 5(2) Indian Journal of Integrated Research in Law 1408.

- Platforms must clearly communicate grievance procedures and ensure users' complaints are addressed within stipulated timelines.

Public-private partnerships in cybercrime prevention.

- Establish multi-stakeholder alliances with law enforcement, intermediary platforms, cybersecurity experts, and civil society for threat intelligence sharing and rapid response.
- Platforms should launch user education initiatives to raise awareness about cyberthreats and safe practices for online engagement.
- Joint development of best practices, standardized reporting templates, and collaborative incident response teams will enhance resilience against cybercriminals.

These measures collectively will improve enforcement capabilities, accountability, and trust among users, intermediaries, and government authorities.

[41] 'Gentle Reminder: DSA Obligations Will Apply to Online Intermediary Services' (National Law Review) (https://natlawreview.com/article/gentle-reminder-dsa-obligations-will-apply-online-intermediary-services-starting-17) accessed 26 October 2025

BIBLIOGRAPHY

BOOKS

- *Cyber Crime, Regulations and Security* (Law Brigade Publishers 2023)
- Podgor ES, 'Cybercrime: National, Transnational, or International?' in *Cybercrime: Law, Enforcement and Society* (Carolina Academic Press 2004)
- Riordan J, 'The Liability of Internet Intermediaries' (DPhil thesis, University of Oxford 2013)
- Talat F, *Cyber Crimes* (3rd edn, Eastern Book Company 2024)

ARTICLES

- Arnell P, 'The Prosecution of Cybercrime – Why Transnational and Extraterritorial Jurisdiction Matter' (2023) International Journal of Law and Information Technology
- 'Cybercrime and Social Media Platforms: Legal and Regulatory Issues' (2023) Law Journal
- Onomrerhinor FA, 'Universal Jurisdiction for Transnational Cybercrimes?' (2023) 3(1) UCC Law Journal
- Peterson JH, 'Global Cyber Intermediary Liability: A Legal & Cultural Comparative Analysis' (2014) 34(1) Pace L Rev 257
- Sorbán K, 'The Role of Internet Intermediaries in Combatting Cybercrime: Organisation and Liabilities' [2019] Central and Eastern European e|Dem and e|Gov Days

ELECTRONIC SOURCES / WEBLIOGRAPHY

- Cambridge University Press, 'Cybercrime - References' accessed 26 October 2025
- JSTOR, 'Document 24479053' [suspicious link removed] accessed 26 October 2025
- Judicial Academy Jharkhand, 'Cyber Crime Cases: Issues, Challenges & Solutions' (2025) https://jajharkhand.in/wp-content/uploads/2025/02/Cyber-Crime-web.pdf accessed 26 October 2025
- 'Liability of Internet Intermediaries and Legal Challenges: A Comprehensive Systematic Review' https://www.researchgate.net/publication/395 accessed 26 October 2025

- OECD, 'The Role of Internet Intermediaries in Advancing Public Policy Objectives' (OECD Publishing 2011) https://www.oecd.org/content/dam/oecd/en/publications/reports/2011/09/the-role-of-internet-intermediaries-in-advancing-public-policy-objectives_g1g13dba/9789264115644-en.pdf accessed 26 October 2025
- Oxford Academic, 'Who are Internet Intermediaries?' in *Internet Intermediaries and the Law* (Oxford University Press 2020) https://academic.oup.com/edited-volume/34234/chapter/29026490 accessed 26 October 2025
- ResearchGate, 'The Role of Internet Intermediaries' https://www.researchgate.net/publication/289773793_The_Role_of_Internet_Intermediaries_in accessed 26 October 2025
- Supreme Court of the United States, 'Slip Opinion 21-1496 (Twitter, Inc. v. Taamneh)' https://www.supremecourt.gov/opinions/22pdf/21-1496_d18f.pdf accessed 26 October 2025
- UNODC E4J, 'Cybercrime Module 7 Key Issues: Sovereignty and Jurisdiction' (2018) https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/sovereignty-and-jurisdiction.html accessed 26 October 2025
- UNODC, 'Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: 2024 Report' (2024) https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf accessed 26 October 2025
- WIPO, 'Internet Intermediaries' https://www.wipo.int/en/web/copyright/internet-intermediaries accessed 26 October 2025