The 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

RESEARCH PAPER

THEME: THE BORDERLESS BATTLEFIELD: REWRITING CRIMINAL LAW FOR A GLOBAL ERA

SUB THEME: CYBER CRIME, DIGITAL EVIDENCE & EXPANDING JURISDICTIONAL BOUNDARIES

TITLE OF SUBMISSION: BLURRING GEOGRAPHICAL BOUNDARIES IN THE AGE OF DIGITAL EVIDENCE & CYBERCRIME

-Malvika Vinod Vachhani

INDEX

ABSTRACT

The traditional tenets which had been followed in establishing criminal jurisdiction have constantly been challenged by the fact that cyberspace is devoid of borders. As cybercrime transcends the geographical borders, the enforcement authorities are scrapped with investigations, prosecutions and trials that are not defined by traditional boundaries. One of the significant obstacles refers to electronically stored information that is scattered across jurisdictions, and as a result, legal arrangements aimed to tackle domestic crimes in regional jurisdictions become inadequate concerning the growing cyberspace.

This study examines the intricate relationship between cybercrime, digital evidence and its borderless framework. In addition to offering solutions, it unfolds the requirements for innovative approaches to jurisdictional cooperation and rule regulation.

The primary objectives of this study are fourfold; First, analysis of the nature and characteristics of digital evidence and cybercrime; Second, Identifying the jurisdictional and procedural challenges faced by court; Third, the necessity of jurisdictional expansion with respect to cross border offences; Fourth, a comparative analysis of India and European jurisdictions to access reform models. The study adopts international conventions, secondary literature, policy frameworks and a doctrinal and comparative research methodology.

The study demonstrates how European legal system has adopted a coordinated response through harmonized procedure standards, cross-border cooperation, specifically under the Budapest Convention and mutual legal assistance, whereas, India continues to face challenges due to extraterritorial data access and institutional capacity. The study further sees how cybercrime adjudication requires a special training for judicial officers and clear rules for governing overseas data access to ensure the integrity of digital evidence.

In addition to this the paper this research contributes to proposing reforms including expanding jurisdictions, modernized procedures and alignment with the international standards, strengthening cybercrime governance and also a robust safeguard for the process and access to justice in this digital age.

CHAPTER 1: INTRODUCTION

In the digital world, cyberspace has emerged as the new frontier of human engagement, business, politics, and online crimes. The constant digitalization of society across the globe has brought fundamental shifts in the way of communicating, financing transactions, and in archiving our data.

Cybercrime, in its very essence, knows no geographical borders, making existing cyberspace laws and even jurisdictions obsolete. Notably, in India, with its bold “Digital India” plan, the country is moving firmly towards becoming an “information society.” However, this advancement is necessarily associated with "unprecedented risks." Starting from identity thefts to ransomware attacks and to massive infiltrations in sensitive data, cyber-criminals have access to and make use of this "interconnected and globalized nature” of the world wide web in ways and means utterly beyond all terrestrial jurisdictions.

But how can legal systems effectively regulate crimes committed in one country and executed in another?

The evolution of cyberspace has compelled legal scholars to rethink the old assumption of criminal jurisdiction, that crime is connected to territory. For years, criminal law has operated on the offences that occur within the geographical boundaries, enabling a robust method to investigate prosecute and punish offenders through clearly defined jurisdictional boundaries. The digital environment however changes this belief and challenges the boundary with a virtual space where neither evidence nor the criminal is confined to one country.

Concepts like territory, nationality and sovereignty continue to dominate criminal law but their application becomes uncertain when crime is mediated through digital spaces. Due to digital expansion, power has shifted from the government to private technological cooperation that holds and can control a vast data pool of private information, communication records and transactional data through cloud-based services across multiple jurisdictions. Since governments need to seek evidence beyond borders in cybercrime, the dependency increases on private entities and introduces a new dimension to criminal justice, where questions of jurisdictions and international regulatory cooperations rise.

This paper will aim at discussing challenges associated both with cybercrime and online evidence in general, by making comparisons between global models like the U.K. Computer Misuse Act, 1990 and Budapest Cybercrime Convention, and evaluate whether the existing models are capable of strengthening international cooperation without compromising on constitutional safeguards. Ultimately, the future of criminal justice cannot merely depend upon one nation alone but upon legal frameworks, an expansion of territorial jurisdiction and a shared global domain with coordinated legal response.

CHAPTER 2: RESEARCH QUESTION & RATIONALE

Digital environment is a space where data moves faster than the law but borders only remain as legal abstractions raising questions about how criminal justice systems legitimately claim jurisdiction over cybercrime and digital evidence and what approaches different countries reveal about the future of sovereignty, accountability and due process in this technological era?

Cybercrime exposes a fundamental paradox of modern law where offences are committed in a borderless space while the accountability still remains anchored to traditional legal systems, these principles are based upon territory, physical presence and fixed geographical evidence that are ill- suited to address crimes in cyberspace. Furthermore, states face ongoing challenges in investigations, evidence collection and prosecution. This is grounded when digital evidence is stored on foreign servers managed by multi technological companies.

India sees a sharp increase in cyber offences as it continues to depend to fragmented legal framework with the Information Technologies Act of 2000, that often fails to address issues and overlaps in authority. However, jurisdictions such as the United States, the European Union and the United Kingdom have a better approach alongside organised responses through judicial principles, laws, international cooperation with rules for accessing data across borders and evolving standards for electronic evidence. While the USA and the EU have significant influence over data flows, platforms and cloud infrastructure countries like India often operate within legal and procedural restrictions set by multinational corporations and foreign legal systems. This imbalance raises key questions about which laws govern cyberspace, how investigative authority is shared across borders and how current jurisdictional principles adequately reflect the realities of digital power rather than just territorial sovereignty.

CHAPTER 3: LITERATURE REVIEW

CHAPTER 3.1: CYBERCRIME

Cybercrime refers to illegal activities facilitated through the internet, these technological advancements in the contemporary era has brought numerous benefits giving rise to a new form of criminal activity known as cybercrime. Cybercrime incorporates a wide range of offences including:

1. Hacking: Unauthorized invasion into computer devices manipulating, accessing and selling digital information
2. Identity Theft: Fraudulent use of personal data impersonating them into financial transactions
3. Online Fraud: Inducing wrongful transfers of money or valuable information.
4. Data Breach: Compromised digital repositories which contribute to unauthorized exploitation of confidential information.

Victims of cybercrime face hardships in reporting incidents, understanding their legal rights and pursuing remedies especially when criminals are located in different countries, casting a multifaced impact on its victims that affect them financially through fraud and unauthorized transactions whose recovery becomes time consuming and costly, involving legal procedures needing prolonged engagement.

Judicial reforms have attempted to address these by introducing victim support units, legal aid mechanisms made to cater to digital crime and online dispute resolution platforms. These measures reflect a global shift towards viewing cybercrime not as a technological problem but as a multifaced institution, legal and social challenge requiring a systematic reform.

CHAPTER 3.2: DIGITAL EVIDENCE

Digital evidence becomes crucial in a digitally mediated world as online transactions and interactions that leave digital footprints make traditional evidence inadequate in capturing information in the cyber-space. Instances involving fraud, terrorist communications, financial transactions make traditional evidence insufficient in capturing the operational realities of cyberspace.

It has largely transformed the functioning of courts in procedural and substantive ways. Courts now rely on digital evidence [also called as electronic evidence] for determining judgements with greater precision; some of which include detailed call records, social media data, cloud data, Meta data and CCTV footage. These accelerate proceedings but raise questions about the authenticity of such evidence, pressurizing courts to develop technological competence, training and interpretation of the digital material.

Although electronic evidence carries weight for precision and acts as a witness, the most prevalent challenge includes lack of set standards for collection and preservation, fundamental complexity faced by experts examining the evidence without such standards and jurisdictional hardships faced due to restricted or cumbersome access on cross-border data. Persistent challenges are also faced with respect to encryption, overload of data that increases the courts' burden, deepfakes and privacy concerns and rights. With these, it is arduous to draw a line between investigation and privacy raising concerns.

Digital evidence has undergone a significant revolution with the rise in artificial intelligence, further increasing complexities in evidence as, AI generates realistic content like deepfakes, blurring the line between authentic and manipulated evidence. This imposes serious challenges to investigators and courts. This demands an evolution in forensic methodologies and strict legal standards.

This type of evidence has become indispensable in nature and exposes the reality of an increasing digital society. Although it offers unprecedented data, it requires a balance between forensic expertise, safeguards and legal standards.

CHAPTER 3.3: NEED FOR EXPANSION IN JURISDICTION

Cyber-offences and digitally generated evidence are stored and registered across multiple jurisdictions for which the reliance on traditional methods resulted in provisions that lacked the unique attributes to address cyber- offending and concreteness of digital evidence. The process for extradition and corporation to get access to data is seen to be complicated due to different data protection regulations, allowing perpetrators to escape justice, disrupting the chain-of-custody protocols that are essential in criminal prosecution.

Digital evidence resides in multiple jurisdictions as it exists in layers, that is, on devices and cloud storage across states. The delay due to permission and protocols that occurs to gain access on this data makes it more vulnerable to altercations. It can additionally be deleted, encrypted or destroyed that may or may not leave a trace. If courts and investigators lack a prompt access to this data across a different jurisdiction, the authenticity and its reliability can be compromised which will further weaken its admissibility and the value it holds.

Perpetrators in this process are faster than a legislation can adapt. Without expanded jurisdiction and legal reforms, these crimes will remain beyond reach despite having digital traces as evidence. The borderless nature of these crimes demands cooperative frameworks among nations including shared investigative tools, treaties and laws.

Sometimes, shared investigative tools and treaties become impossible to exist among nations due to conflicted perspectives and historical conflicts. Hence, here International Laws and Conventions play an important role as they can provide for standardized legal procedures and laws applicable across nations allowing cooperation and preservation of crucial evidence the failure to comply with which shall result in diplomatic pressure, trade restrictions and exclusion from international cooperation via international law governing bodies. These will bind nations to preserve and share access to data to other jurisdiction, eradicating cyber-offences.

When the question about authenticity is raised, legal systems have adopted reforms including reshaping the role of experts to access such situations that are necessary for relying on digital evidence preventing wrongful convictions derived from altered data. With dispersed jurisdiction of crimes, questions arise with respect to cross border data access.

Despite adopting such reforms to address online crimes, the existing framework fails to entirely comply with the nature of these crimes and as these issues multiply across networks compared to physical locations, we observe the need for expansion of jurisdictional boundaries as a central legal challenge along with classification and evidence issues.

Without substantial action in accordance with jurisdiction, the fight against cybercrime will remain ineffective and fragmented. This highlights the urgent need for expansion of jurisdiction and international cooperation to restrict the rapid growth of online crimes.

CHAPTER 4: ANALYSIS OF EXISTING INDIAN LAWS THROUGH A COMPARATIVE LENS WITH FOREIGN NATIONS

CHAPTER 4.1: ANALYSIS OF EXISTING INDIAN LAWS

The admissibility of digitally acquired evidence in India is governed by the Indian Evidence Act of 1872 that has now changed to the new Bharatiya Sakshya Adhiniyam, 2023. This act recognises digital evidence as electronic records in Section 63, laying down conditions for such evidence to be admissible in courts. This includes an accurate data from devices as per the rule in Section 63(2) that further states the importance of the computer output being regularly used by a person with lawful control of that device being properly functional and the accurate reproduction of the information fed during its ordinary use.

India constantly develops jurisprudence around the admissibility, reliability and the requirement for proper chain of custody in addition to forensic examination. The initiatives of setting up cyber forensic laboratories nationwide to cater to digital evidence has proved to be beneficial. The Indian government also actively coordinates and cooperates internationally by signing Memorandum of Undertaking with other countries for easy access to cross-border data required to combat cyber-crimes. Additionally, awareness initiatives are also undertaken to educate the citizens about safe online practices and reporting tools. However, challenges pertaining to advanced forensic technique to effectively handle digital evidence, jurisdictional disparities and availability of qualified experts still need to be catered to.

Another approach to combat these issues within the jurisdiction of India is the Information and Technology Act of 2000 that laid the foundation for cyber law and is seen as a landmark legislation that addresses such digital crimes such as cyber-terrorism, identity theft, publication of obscene material online and hacking.

The Data Protection Bill of 2019 is observed as a bill that serves to safeguard personal information and responsibility of handling such crucial data. It establishes norms for data preservation and access by public and private entities, regulate privacy and grants the Government to exempt certain investigating agencies in matters involving national security and public order.

This bill and its several drafts underwent reviews by the parliamentary committee but did not succeed in becoming a law, yet the Digital Personal Data Protection Act enacted by the parliament in India in 2023 effectively replaces this bill and its objectives with this Act.

The new act aims to maintain a balance between individual privacy rights on personal data and the needs of government agencies to process this data for necessary purposes. Further, the Data Protection Board of India acts as a surveillance and addresses grievances. This act includes processing of personal data with prior consent protecting privacy rights; To ensure this process penalties are imposed upon officers for any breach of the rule. This also applies to data outside the jurisdiction of this country in cases of offering goods and services to individuals in India, that is, foreign entities can be held accountable for wrongly handling data of Indian citizens and will be brought within the Indian jurisdiction. This will ensure accountability beyond the jurisdiction of India.

CHAPTER 4.2: COMPARATIVE STUDY WITH THE LAWS OF THE UNITED KINGDOM

The United Kingdom's framework for fighting cybercrime, especially under the Computer Misuse Act, 1990, can be regarded as more effective and advanced in comparison to the present framework of law in the Indian context under the Information Technology Act, 2000. The first major advantage of the United Kingdom statute would be its specificity or precision in defining crimes. It can thus be understood that the United Kingdom's Computer Misuse Act in its precise approach clearly defines crimes such as unauthorized access to computer systems or data, access with the intention of committing further crimes, or unauthorized amendment of data.

Further, the UK also has continuing updates to its legislation to cater to new-age threats, such as additions to the offense about serious damage, security, and critical infrastructure. India, as a comparison, still relies heavy-handedly on the IT Act, 2000, which was written during the early stages of the digital age and fails to define new-age crimes, such as ransomware, massive identity fraud, and cryptocurrency frauds.

Thus, even while India has made significant changes strengthening its laws to combat cybercrimes, United Kingdoms' Legal aspects and rules reveal a technologically evolved approach that can be adapted by India for a progressive approach

CHAPTER 4.3: COMPARATIVE STUDY WITH EUROPEAN LAWS

The Budapest Convention on Cybercrime of 2001, adopted within the Council of Europe, remains the first international agreement that is exhaustive in its scope for combating cybercrime. It aims to provide a universal framework of law for the harmonization of domestic legislation in member states related to crimes committed online in a bid to ensure that crimes such as hacking, fraud, data abuse, and identity theft are criminalized in all of the member states. Except these, issues of substantive law, the Budapest Convention of 2001 also puts emphasis on the need for improvement in the procedural side of law with the aim to ensuring that law enforcers in the member states are endowed with contemporary methods for the preservation, collection, and admissibility of computer-based evidence in investigations. This entails the need for rapid data preservation assistance in addition to the need for the real-time collection of traffic data as well as the requirement for the interception of lawfully requested communications. Additionally, the need for international cooperation also takes prominence in the Budapest Convention of 2001.

In India, cybercrimes are governed by the Information Technology Act of 2000 and provisions of the BNS and BSA of 2023, dealing with all other crimes like hacking, identity theft, cyber terrorism, and online fraud. However, a harmonized global act like the Budapest Convention addresses a variety of issues like international collaboration at a much faster pace. It provides a platform for all the Nations to take joint initiatives against the global issue of cybercrime swiftly.

CHAPTER 5: OBSERVATION AND SUGGESTION

India shall draw valuable lessons from the UK's cybercrime laws and develop the more effective laws. Ensuring proportionate punishment and a sense of clear enforcement in this regard along with improvement in the procedural aspects in the field of investigation and preservation and update the laws from time to time to incorporate the new threats in technology on constant basis. Constant upgradation in laws will result harmony in the Indian laws as well as international laws in this field.

Being one of the major victims of cybercrime, India has not yet joined the Budapest Convention. The main reasons for India's reservation include sovereignty concerns, data jurisdiction issues and preference for domestic legislation rather than one that caters solely to developed countries.

The essence of cybercrime knows no border: offenders operate most of the time from foreign jurisdictions, beyond the reach of local laws. It is favorable and advisable for India to sign the Budapest Convention as it would help achieve faster cross-border investigations, improve evidence sharing mechanism help harmonize Indian cyber laws with global standards, strengthening India’s global standing on Cyber Diplomacy and provide domestic enforcement agencies with international tools

Most notably, countries like the USA and Israel, with whom India already cooperates bilaterally, are signatories to the Convention weakening India's justification for staying out.

CHAPTER 6: RESEARCH GAP

The research gap in this study could involve the following reasons:
Resource Constraints: Due to resource limitations, some aspects might not be completely addressed within this study.
Dynamic Nature of Cyber Threats: The ever-dynamic nature of cyber threats causes difficulties in offering real-time insights.

CHAPTER 7: CONCLUSION

Currently the digital age has dramatically altered the landscape of crime and crime-solving, which has made it evident that national laws are insufficient for dealing with problems that are not confined within territorial boundaries. The Indian law and policy structure, although constantly growing under the draconian conditions of the IT Act, 2000; BNS, 2023; and Digital Personal Data Protection Bill, 2023, is yet to find smooth ways of dealing directly with international challenges. The act of closely analysing the effective and specific legislation adopted by the United Kingdom and the international agreements embodied under the Budapest Convention prepares the Indian government to take a dual strategy to deal with the challenges of advancements in technology. Joining the Budapest Convention will not only be helpful for the Indian government to deal effectively with cybercrime but will also be a way for the country to be an active part of the global community dealing with cyberspace. In a world where footprints in cyberspace are as real as footprints in reality, it is not a matter of choice to have effective cyber legislation; rather, it is the need of the hour.

REFERENCES

1. Challenges to Indian Law and Cyber Crime Scenario in India. (2025). Law Gratis.
2. Parliament. (2023). THE BHARATIYA SAKSHYA ADHINIYAM, 2023 [Legislation]. THE GAZETTE OF INDIA EXTRAORDINARY, N–O. 47. https://www.mha.gov.in/sites/default/files/250882_english_01042024.pdf
3. Parliament. (2023b). THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023. In THE GAZETTE OF INDIA EXTRAORDINARY. https://prsindia.org/files/bills_acts/bills_parliament/2023/Digital_Personal_Data_Protection_Act,_2023.pdf
4. International Journal of Research and Analytical Reviews (IJRAR), 10(3), 183–197. https://ssrn.com/abstract=4789133
5. International Journal of Legal Education and Research (IJLER), 1(2).
6. International Journal of Scientific Interdisciplinary Research, 5(2), 1–29. https://doi.org/10.63125/960x9767
7. Kerr, O. S. (2005). Digital evidence and the new criminal procedure. Harvard Law Review, 119(1), 279–366.