



INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL**
**ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

CYBERCRIME AND JURISDICTIONAL CHALLENGES: EXTRATERRITORIAL APPLICATION OF CRIMINAL LAW IN CROSS- BORDER CYBER OFFENCES

AUTHORED BY - HARSIMRAN SINGH HARRY

LLM Student

CO-AUTHOR - DR. CHEENA ABROL

Assistant Professor, CT University, Ludhiana

ABSTRACT

Cybercrime is the paradigm borderless offence: a perpetrator in one State may deploy malware through servers in a second, defraud victims in a third, and store the proceeds on a cloud platform controlled by a company incorporated in a fourth. Criminal law, by contrast, remains tethered to the territorial State. This paper examines how that tension is managed through the extraterritorial application of criminal law. It first sets out the public international law foundations of prescriptive, adjudicative and enforcement jurisdiction and tests the traditional bases of jurisdiction against the architecture of cyberspace. It then analyses the Indian framework, namely sections 1(2) and 75 of the Information Technology Act, 2000, section 1 of the Bharatiya Nyaya Sanhita, 2023 and the procedural provisions of the Bharatiya Nagarik Suraksha Sanhita, 2023, together with the leading judicial pronouncements. A comparative study of the United States, the United Kingdom, the European Union, Canada and Australia follows, as does an evaluation of the Budapest Convention, its Second Additional Protocol and the recent United Nations Convention against Cybercrime. The paper argues that while India possesses broad prescriptive reach, its adjudicative and enforcement capacity is constrained by procedural gaps, reliance on slow mutual legal assistance and the absence of a clear framework for cross-border electronic evidence. It concludes with a set of doctrinal and institutional recommendations.

Keywords: *cybercrime; jurisdiction; extraterritoriality; cross-border data; Information Technology Act, 2000; Bharatiya Nyaya Sanhita, 2023; Budapest Convention; mutual legal*

assistance; effects doctrine.

I. INTRODUCTION

The Westphalian settlement assigns to each State authority over persons, things and events within its territory. Criminal law has historically followed that logic: a crime is investigated where it is committed, prosecuted by the courts of that place and punished under its law. The internet unsettles each step of this reasoning. A single phishing campaign, ransomware attack or online financial fraud can involve a perpetrator, a victim, an intermediary, a server and a payment channel in different countries, each of which may plausibly claim a legitimate interest in prosecuting the offence.¹

The resulting difficulty is not merely theoretical. It determines whether an Indian victim of a fraud orchestrated from abroad can obtain justice, whether Indian investigators may compel a foreign platform to produce data, and whether a foreign national who attacks critical Indian infrastructure from beyond Indian borders can be tried in India. Three distinct questions are entangled in such cases. The first is whether a State has the legal competence to make its criminal law apply to conduct abroad (prescriptive jurisdiction). The second is whether its courts may try the accused (adjudicative jurisdiction). The third is whether its officials may lawfully act, whether by arrest, search or seizure, outside their own territory (enforcement jurisdiction). Much confusion in the literature and in practice arises from treating these as one.²

A. Research Problem

Although India has legislated for extraterritorial reach in cyber matters since 2000, the actual capacity of Indian courts and agencies to prosecute cross-border cyber offences remains uncertain. Statutory reach has outpaced procedural machinery, and international instruments that might fill the gap have either not been joined by India or are yet to mature.

B. Research Objectives

- To explain the international law principles governing criminal jurisdiction and assess their adaptability to cyberspace.
- To analyse the extraterritorial provisions of Indian law applicable to cyber offences and

¹See generally Susan W Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Praeger 2010); Jonathan Clough, *Principles of Cybercrime* (2nd edn, Cambridge University Press 2015) ch 10.

²Cedric Ryngaert, *Jurisdiction in International Law* (2nd edn, Oxford University Press 2015) 5-12.

the manner in which courts have applied them.

- To compare approaches adopted in major foreign jurisdictions and in international instruments.
- To identify gaps in the Indian framework and propose workable reforms.

C. Research Questions

- Are the traditional bases of criminal jurisdiction adequate for cross-border cyber offences?
- How far does Indian law validly and effectively extend to offences committed outside India?
- What obstacles prevent the translation of prescriptive reach into successful prosecution?
- What legal and institutional reforms would best reconcile State sovereignty with effective cross-border enforcement?

D. Research Methodology

This study adopts a doctrinal and analytical methodology. Primary sources comprise statutes, treaties and judicial decisions; secondary sources comprise treatises, scholarly articles and reports of international bodies. Comparative analysis is employed selectively, confined to jurisdictions whose practice has shaped global debate. The paper does not rely on empirical data, and statistical claims have been avoided in preference to doctrinal analysis.

II. JURISDICTION IN INTERNATIONAL LAW: THE CONCEPTUAL FOUNDATION

A. The Lotus Principle and Its Limits

The starting point of any inquiry into extraterritorial jurisdiction is the decision of the Permanent Court of International Justice in the *S.S. Lotus* case.³ The Court held that international law does not prohibit a State from extending its criminal law to acts abroad unless a prohibitive rule can be identified; restrictions on territorial reach, however, are strict as regards enforcement. That permissive reading has been qualified by later practice, which insists on a genuine connection between the State and the offence, and by the principle of non-intervention. In the cyber context the permissive approach has had a double effect: it gives

³*The Case of the S.S. Lotus (France v Turkey)* (1927) PCIJ Series A No 10.

States wide latitude to legislate, and it multiplies the number of States with a lawful claim to the same conduct.

B. Recognised Bases of Jurisdiction

The Harvard Research Draft Convention on Jurisdiction with Respect to Crime (1935) identified five principal bases, which continue to structure the analysis.⁴ Table 1 summarises each and its application to cyberspace.

Table 1: Bases of Criminal Jurisdiction and Their Cyber Application

Principle	Basis of claim	Cyber application	Principal limitation
Territorial (subjective and objective)	Offence commenced, or consummated/producing effects, within the territory	Attack launched from, or effects felt in, a State; location of servers or victims	Indeterminate locus of acts; many States may claim "effects"
Nationality (active personality)	Offender is a national	Nationals committing cyber offences from anywhere	Does not reach foreign offenders; requires double criminality in some systems
Protective	Threat to the State's security or vital interests	Attacks on critical infrastructure, state data, currency, cyber terrorism	Risk of overbroad claims to "national interest"
Passive personality	Victim is a national	Online fraud, harassment, identity theft targeting citizens	Controversial; weakens predictability for offenders
Universality	Offence is of universal concern	Online child sexual abuse material, arguably	Confined to a narrow class of crimes; not settled for ordinary cybercrime

The objective territorial principle, together with its offshoot the effects doctrine, has been the

⁴Harvard Research in International Law, *Draft Convention on Jurisdiction with Respect to Crime* (1935) 29 AJIL Supp 435.

most consequential in the digital environment. Its classic formulation is found in *United States v Aluminum Co of America*,⁵ and its application to cyber offences was confirmed in *United States v Ivanov*, where a Russian national who accessed a Connecticut-based company's systems from Russia was held amenable to American jurisdiction.⁶ The English House of Lords reached an analogous outcome in the extradition proceedings against Vladimir Levin, who had transferred funds from a New York bank by keyboard commands issued in St Petersburg; the acts were treated as having been done where the computer in New York was affected.⁷

C. Why Cyberspace Strains the Doctrine

The traditional principles presuppose that conduct, effects and persons can be located. Cyberspace complicates each presupposition. Data is divisible, mobile and replicated; routing is determined by network efficiency, not geography; and cloud providers often store fragments of a single user's data in several States. Scholars have therefore described data as "un-territorial", arguing that location of data is an increasingly poor proxy for the jurisdictional interests at stake.⁸ The Tallinn Manual 2.0, though addressed to State conduct in cyberspace generally, recognises territorial and extraterritorial jurisdiction over cyber activities but affirms that enforcement remains confined by the territorial sovereignty of other States.⁹

III. JURISDICTIONAL CHALLENGES IN CROSS-BORDER CYBER OFFENCES

A. Attribution and Anonymity

Jurisdiction cannot be exercised until the offender is identified. Use of virtual private networks, anonymising routers, compromised third-party machines and cryptocurrency mixers frustrates both technical and legal attribution. The problem is intensified where the offender is acting through botnets spread across dozens of jurisdictions, so that the machines used are located in States with no connection to the principal wrongdoer.

B. Concurrent Jurisdiction and Conflict of Laws

When more than one State legitimately asserts jurisdiction, three consequences follow:

⁵*United States v Aluminum Co of America*, 148 F 2d 416 (2d Cir 1945).

⁶*United States v Ivanov*, 175 F Supp 2d 367 (D Conn 2001).

⁷*R v Governor of Brixton Prison, ex p Levin* [1997] AC 741 (HL).

⁸Jennifer Daskal, "The Un-Territoriality of Data" (2015) 125 Yale LJ 326.

⁹Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017) rr 9-10.

duplication of proceedings, tension between inconsistent legal standards and the risk of violating the *ne bis in idem* norm. Conduct that is a serious offence in one State, such as certain categories of speech, may be lawful in another. Corporate platforms may thus be placed in a position where compliance with one State's order necessarily constitutes breach of another's law, a problem sharply illustrated in the American litigation concerning *Yahoo!* and the French courts.¹⁰

C. Location and Ownership of Electronic Evidence

Electronic evidence is volatile, may be overwritten in days or hours, and is frequently held by service providers established abroad. The question whether a State can compel a provider within its jurisdiction to produce data stored overseas was at the centre of *Microsoft Corp v United States*, in which the Second Circuit refused to enforce a warrant under the Stored Communications Act for emails stored in Ireland.¹¹ The United States Congress responded with the Clarifying Lawful Overseas Use of Data (CLOUD) Act of 2018, which links the reach of a warrant to the provider's "possession, custody, or control" of the data, irrespective of its location.¹² The episode shows the shift from a territorial to a control-based model of data jurisdiction.

D. Dual Criminality and Extradition

Extradition and mutual legal assistance traditionally require dual criminality, that is, the conduct must be an offence in both the requesting and requested States. Because cybercrime laws vary widely in scope, definitions and penalties, dual criminality can prove an obstacle even among friendly States. Extradition proceedings are also slow, a particular concern where evidence will be lost long before the proceedings end.

E. The Role of Intermediaries

Internet intermediaries are both gatekeepers of evidence and potential enforcement points. Questions of whether a State may compel a platform to remove content globally, as opposed to geographically, raise acute jurisdictional questions that courts around the world have answered inconsistently, as discussed in Part V below.

¹⁰*Yahoo! Inc v La Ligue Contre Le Racisme et L'Antisemitisme*, 433 F 3d 1199 (9th Cir 2006) (en banc).

¹¹*Microsoft Corp v United States*, 829 F 3d 197 (2d Cir 2016), vacated as moot, *United States v Microsoft Corp*, 138 S Ct 1186 (2018).

¹²Clarifying Lawful Overseas Use of Data Act 2018 (Pub L 115-141, Div V), codified at 18 USC s 2713.

IV. THE INDIAN LEGAL FRAMEWORK

A. Statutory Provisions on Extraterritorial Reach

The Information Technology Act, 2000 (IT Act) is the principal cyber statute in India. Its extraterritorial reach rests on two provisions. Section 1(2) declares that, save as otherwise provided, the Act applies also to any offence or contravention committed outside India by any person. Section 75 elaborates this: the Act applies to an offence or contravention committed outside India by any person, irrespective of nationality, if the act constituting it involves a computer, computer system or computer network located in India.¹³ The legislature has thus adopted the objective territorial principle, anchored on the situs of the computer resource and not on the nationality of the offender or the victim.

The general criminal law has been brought into harmony with this. Section 1 of the Bharatiya Nyaya Sanhita, 2023 (BNS), which replaced the Indian Penal Code, 1860, preserves the earlier position that Indian citizens committing offences anywhere in the world are liable under it, and extends the Sanhita to any person committing an offence beyond India that targets a computer resource located in India.¹⁴ Section 48 of the BNS likewise punishes abetment in India of offences committed outside India, corresponding to section 108A of the earlier Code.

Several substantive IT Act offences have particular transnational relevance. Section 43 and section 66 address unauthorised access, data theft, introduction of malware and denial of service; section 66C and section 66D penalise identity theft and cheating by personation using a computer resource; and section 66F deals with cyber terrorism, the offence in which the protective principle is most clearly engaged. Section 81 provides that the IT Act overrides inconsistent provisions of other laws, a point of importance when overlapping offences such as obscene publication arise under both the IT Act and general penal law.¹⁵

B. Judicial Approach to Offences with Foreign Elements

Indian courts developed the jurisdictional framework for transborder offences well before the IT Act. In *Mobarik Ali Ahmed v State of Bombay*, the Supreme Court sustained the trial of a foreign national who, from outside India, fraudulently induced Indian parties to part with property, holding in substance that the offence was consummated in India where its effects were felt.¹⁶ In *Ajay Agarwal v Union of India*, the Court recognised that a conspiracy hatched

¹³Information Technology Act 2000, ss 1(2), 75(1)-(2).

¹⁴Bharatiya Nyaya Sanhita 2023, s 1(4)-(5), corresponding to Indian Penal Code 1860, ss 3-4 (the latter as amended by the Information Technology Act 2008).

¹⁵*Sharat Babu Digumarti v Government of NCT of Delhi* (2017) 2 SCC 18.

¹⁶*Mobarik Ali Ahmed v State of Bombay* AIR 1957 SC 857.

abroad but with acts in pursuance of it in India, and with continuing effects, could be tried by Indian courts.¹⁷ These decisions apply the objective territorial and effects principles and supply a doctrinal bridge from physical to digital offences.

On internet-specific disputes, the Delhi High Court in *Banyan Tree Holding (P) Ltd v A Murali Krishna Reddy* adopted a "purposeful availment" standard for determining whether a forum court may exercise jurisdiction over a foreign website operator: mere accessibility of a website in India is insufficient, and there must be targeting of the Indian forum with consequences within it.¹⁸ Although rendered in a civil context, this reasoning parallels the "targeting" test applied internationally and offers a useful limiting principle against indefinite criminal reach. In relation to platform liability, the Supreme Court in *Shreya Singhal v Union of India* read down the intermediary takedown obligation in section 79 so that it is triggered by a court order or governmental notification, and upheld the blocking regime in section 69A with its procedural safeguards.¹⁹ The Delhi High Court, in *Swami Ramdev v Facebook Inc*, directed global removal of content that had been found unlawful in India, reasoning that content uploaded from India and accessible worldwide could be disabled globally if the intermediary has the technical means to do so.²⁰ The decision aligns India with a growing line of authority recognising worldwide injunctions, but it has also invited the criticism, examined below, that unilateral global orders risk comity conflicts and a "race to the bottom" in free expression.

C. Electronic Evidence and Cross-Border Proof

Prosecution of cross-border offences depends on admissibility of electronic records. Under the Bharatiya Sakshya Adhiniyam, 2023 (BSA), section 63 now governs the admissibility of electronic records, continuing the certificate regime of section 65B of the Indian Evidence Act, 1872, as interpreted in *Anvar P V v P K Basheer* and *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*.²¹ Where the data originates abroad, procuring the requisite certificate from a foreign service provider may itself be impeded by the very jurisdictional obstacles discussed above. The Supreme Court has been receptive to the use of video-conferencing for examining witnesses located abroad,²² but the recording of evidence abroad remains reliant on letters of request.

¹⁷*Ajay Agarwal v Union of India* (1993) 3 SCC 609.

¹⁸*Banyan Tree Holding (P) Ltd v A Murali Krishna Reddy* (2010) 42 PTC 361 (Del) (DB).

¹⁹*Shreya Singhal v Union of India* (2015) 5 SCC 1.

²⁰*Swami Ramdev v Facebook Inc* (Delhi HC, 23 October 2019).

²¹*Anvar P V v P K Basheer* (2014) 10 SCC 473; *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1; Bharatiya Sakshya Adhiniyam 2023, s 63.

²²*State of Maharashtra v Dr Praful B Desai* (2003) 4 SCC 601.

D. Procedural Machinery and Enforcement Mechanisms

Reach in substance is not matched by clarity in procedure. Five features deserve attention.

- *Sanction and forum for offences abroad.* Section 208 of the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), the successor to section 188 of the Code of Criminal Procedure, 1973, provides that offences committed outside India by a citizen, or by any person on an Indian registered ship or aircraft, may be inquired into and tried as if committed where the accused is found, but only with the previous sanction of the Central Government.²³ The provision does not expressly address a foreign national who targets an Indian computer resource under section 75 of the IT Act, leaving it open to argument whether the sanction requirement applies and which court is competent.
- *Extradition.* Extradition is governed by the Extradition Act, 1962 and bilateral treaties. Many older treaties list offences by category and do not clearly cover cyber offences, so reliance must be placed on the dual criminality principle or on the general "conduct" language of newer treaties.
- *Mutual legal assistance.* India has concluded mutual legal assistance treaties with a number of States, including the United States (2005). The BNSS contains provisions on letters of request to courts abroad and on reciprocal arrangements for assistance in criminal matters, successors to sections 166A and 105A-105L of the earlier Code.²⁴ In practice the formal process is slow relative to the lifespan of volatile data.
- *Interception, blocking and intermediary compliance.* Sections 69, 69A and 69B of the IT Act and their rules empower the Government to direct interception, monitoring, decryption and blocking, and the CERT-In directions issued in April 2022 under section 70B(6) impose time-bound incident reporting and log-retention obligations on service providers, including those with foreign operations.²⁵ These domestic tools can only reach entities with an Indian presence or reachable assets.
- *Institutional coordination.* The Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs and the National Cybercrime Reporting Portal provide a centralised national interface, but the proportion of complaints involving offenders abroad necessarily depends on international cooperation.

²³Bharatiya Nagarik Suraksha Sanhita 2023, s 208.

²⁴Bharatiya Nagarik Suraksha Sanhita 2023, Chapter VIII (including s 112 on letters of request); cf Code of Criminal Procedure 1973, ss 105A-105L, 166A.

²⁵Information Technology Act 2000, ss 69, 69A, 69B, 70B(6); Ministry of Electronics and Information Technology, CERT-In Directions dated 28 April 2022.

E. Data Protection and Extraterritoriality

The Digital Personal Data Protection Act, 2023 also adopts an extraterritorial provision, applying to processing of digital personal data outside India if it is in connection with offering goods or services to data principals within India.²⁶ Although regulatory and not penal in the strict sense, it represents a second pillar of India's "targeting"-based approach and one that is converging with the GDPR model discussed below.

V. COMPARATIVE PERSPECTIVES

Table 2 summarises the jurisdictional strategies of selected jurisdictions, and the sections that follow discuss the most instructive features.

Table 2: Selected Comparative Approaches

Jurisdiction	Key instrument / authority	Approach
United States	Computer Fraud and Abuse Act; CLOUD Act 2018; <i>Ivanov</i>	Effects-based territorial reach; "protected computer" includes those used in or affecting foreign commerce; control-based access to data held by US providers
United Kingdom	Computer Misuse Act 1990, ss 4-5; <i>Levin</i>	"Significant link" test: either the accused or the targeted computer must be in the UK at the relevant time
European Union	GDPR Art 3; <i>Google v CNIL</i> ; <i>Glawischnig-Piesczek</i>	Targeting criterion for data protection; global orders possible in defamation cases but not mandated for delisting
Canada	<i>Google Inc v Equustek Solutions Inc</i> 2017 SCC 34	Courts may grant worldwide interlocutory injunctions against non-party intermediaries where necessary for effective relief
Australia	<i>Dow Jones & Co Inc v Gutnick</i> (2002) 210 CLR 575	Online publication is located where it is downloaded and comprehended, exposing publishers to multiple fora

²⁶Digital Personal Data Protection Act 2023, s 3(b).

A. United States and United Kingdom

The United States has long applied a broad effects doctrine. The Computer Fraud and Abuse Act defines a "protected computer" to include one used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States where used in a manner that affects American commerce or national security.²⁷ The United Kingdom's Computer Misuse Act 1990 takes a more calibrated approach. Sections 4 and 5 require at least one "significant link" with the domestic jurisdiction, either that the accused was in the United Kingdom when the act was done or that the targeted computer was there.²⁸ India's section 75 resembles the second limb of the United Kingdom test, but unlike it does not provide an express catalogue of what counts as a link or a mechanism to avoid duplicative prosecution.

B. The European Union

The Court of Justice of the European Union has adopted a nuanced stance on global reach. In *Google Spain* it applied EU data protection law to a search engine operator on the basis of its establishment in a Member State.²⁹ In *Google v CNIL* the Court held that EU law does not require a search engine operator to carry out de-referencing on all versions of its search engine worldwide, though it did not prohibit national authorities from ordering such measures where justified under national standards,³⁰ whereas in *Glawischnig-Piesczek v Facebook Ireland* it held that EU law does not preclude injunctions with worldwide effect in respect of identical or equivalent defamatory content, provided they remain within the framework of relevant international law.³¹ The Article 3(2) GDPR targeting criterion is a further model of principled extraterritoriality.

C. Canada and Australia

In *Equustek* the Supreme Court of Canada upheld a worldwide injunction against Google, reasoning that an order limited to Canadian domains would be ineffective and that the order's impact on comity and free expression was not demonstrated to be unjustified.³² In *Gutnick*, the High Court of Australia held that defamation by internet publication occurs where the material is downloaded, a rule which, if extended to criminal liability, could produce nearly universal

²⁷Computer Fraud and Abuse Act, 18 USC s 1030(e)(2).

²⁸Computer Misuse Act 1990 (UK), ss 4-5.

²⁹Case C-131/12 *Google Spain SL v Agencia Espanola de Proteccion de Datos* [2014] ECLI:EU:C:2014:317.

³⁰Case C-507/17 *Google LLC v Commission nationale de l'informatique et des libertes (CNIL)* [2019] ECLI:EU:C:2019:772.

³¹Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Ltd* [2019] ECLI:EU:C:2019:821.

³²*Google Inc v Equustek Solutions Inc* 2017 SCC 34.

jurisdiction.³³ The contrast between *Equustek* and the CJEU's reasoning in *CNIL* shows an unresolved debate between effectiveness and comity.

D. Lessons for India

Three lessons emerge. First, effective regimes combine a targeting or "significant link" filter with clear reach for control over data. Second, global orders require articulated proportionality and comity safeguards. Third, executive agreements and treaty frameworks are indispensable complements to unilateral extraterritorial legislation. The Indian position, which is broad on reach but thin on filters and safeguards, would benefit from borrowing each.

VI. INTERNATIONAL INSTRUMENTS AND COOPERATION

A. The Budapest Convention and Its Second Additional Protocol

The Council of Europe Convention on Cybercrime (Budapest Convention), opened for signature in 2001 and in force since 2004, remains the most influential multilateral instrument. It harmonises substantive offences, establishes procedural powers such as expedited preservation of data, and provides for international cooperation.³⁴ Article 22 requires parties to establish jurisdiction on territorial and, in specified conditions, nationality grounds, and provides for consultation where more than one party asserts jurisdiction over the same offence. Article 32 permits transborder access to stored data without the authorisation of another party in limited circumstances, namely where the data is publicly available or where lawful and voluntary consent is obtained. The Second Additional Protocol of 2022 adds mechanisms for direct cooperation with service providers in other parties, emergency mutual assistance and joint investigation teams.³⁵

India is not a party to the Convention. The reasons commonly attributed to India's position include its non-participation in the original drafting and concerns, particularly regarding Article 32, that the transborder access provisions may compromise sovereignty. These concerns are intelligible, but non-accession carries real costs: Indian authorities are excluded from the Convention's 24/7 contact network and from streamlined channels for expedited data preservation.

³³*Dow Jones & Co Inc v Gutnick* (2002) 210 CLR 575.

³⁴Convention on Cybercrime (Budapest, 23 November 2001) ETS No 185.

³⁵Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence (opened for signature 12 May 2022) CETS No 224.

B. The United Nations Convention against Cybercrime

After several years of negotiation by an Ad Hoc Committee, the United Nations General Assembly adopted a Convention against Cybercrime in December 2024, which was opened for signature in 2025.³⁶ The instrument has a broader membership base than the Budapest Convention and covers both cyber-dependent offences and the collection of electronic evidence for serious crimes generally. It has also attracted criticism from civil society and some governments over the breadth of its evidence-sharing powers and the adequacy of its human rights safeguards. For India, it presents a more politically acceptable multilateral vehicle than Budapest, and the question for policymakers is whether and on what reservations to join.

C. Bilateral and Informal Cooperation

Mutual legal assistance treaties, INTERPOL notices and police-to-police channels remain the practical backbone of cross-border enforcement. Their chief weakness is speed. Executive agreements of the kind contemplated by the CLOUD Act, under which qualifying foreign governments can request data directly from United States providers, present a potentially useful model for India, subject to adequate rule-of-law and privacy safeguards.

VII. CRITICAL ANALYSIS

The foregoing survey supports four principal conclusions.

First, prescriptive reach is not the real problem. India's statutes already reach foreign offenders targeting Indian computer resources, and the Supreme Court's reasoning in *Mobarik Ali* and *Ajay Agarwal* supplies a robust doctrinal base. The central deficiency lies in adjudicative and enforcement capacity. A law that purports to apply to a foreign hacker is of little use if the hacker cannot be identified, located, arrested or extradited.

Second, the locus-of-computer test is both over- and under-inclusive. Section 75 turns on the location of a computer, computer system or network in India. This captures many attacks but may fail where the victim is an Indian citizen or entity whose data is hosted on foreign infrastructure, and the cloud makes such scenarios increasingly common. Conversely, a foreign attacker's incidental use of an Indian server as a relay could trigger jurisdiction over conduct with no meaningful Indian impact. A test oriented to the targeting of Indian persons or interests,

³⁶UNGA Res 79/243 (24 December 2024), adopting the United Nations Convention against Cybercrime; strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes. The current status of signatures and ratifications should be verified before reliance.

combined with a substantial-effect requirement, would be more principled and more predictable.

Third, unilateral global orders carry comity costs. The Delhi High Court's reasoning in *Ramdev* is understandable from the perspective of effective remedy, but it invites reciprocal claims by other States to dictate what Indian users may see. Without a doctrine of restraint, a proportionality standard and an opportunity for foreign intermediaries to show conflict of laws, such orders risk undermining both free expression and cooperative enforcement.

Fourth, evidentiary and procedural gaps jeopardise prosecutions. The certification requirement under section 63 of the BSA, the absence of express procedures for direct requests to foreign providers and the doubts surrounding the sanction regime for foreign offenders under the BNSS combine to create uncertainty for investigators and defence counsel alike. Such uncertainty also bears on the accused's rights, since vague or unpredictable assertions of jurisdiction may fall foul of the guarantee of fair procedure under Article 21 of the Constitution of India.

VIII. SUGGESTIONS AND RECOMMENDATIONS

- *Refine the jurisdictional nexus.* Amend section 75 of the IT Act to supplement the location-of-computer test with a "significant link" or targeting standard (covering offences directed at persons, entities or critical information infrastructure in India), and add a requirement of substantial effect in India.
- *Clarify procedure for foreign offenders.* Amend the BNSS to specify the competent court, the investigating agency and whether Central Government sanction is required for offences under section 75 of the IT Act committed by non-citizens abroad, so that procedure is aligned with substantive reach.
- *Create a statutory framework for cross-border electronic evidence.* Enact provisions authorising preservation orders, production orders to providers with a substantial presence in India regardless of where data is stored, and direct-request mechanisms, with judicial authorisation and proportionality safeguards.
- *Pursue international instruments strategically.* Evaluate signature of the United Nations Convention against Cybercrime with appropriate reservations; consider observer participation or accession to the Budapest framework, particularly the Second Additional Protocol; and negotiate executive agreements with major data-hosting States.

- *Expedite mutual legal assistance.* Establish a dedicated cyber desk within the nodal authority for MLATs, with fixed timelines, standard templates and a 24/7 contact point, and strengthen capacity within the I4C.
- *Adopt comity and proportionality guidelines for global orders.* Judicial and executive orders with extraterritorial effect should be justified by necessity, narrowly tailored and accompanied by an opportunity for affected intermediaries to demonstrate conflicts with foreign law.
- *Update extradition practice.* Adopt "conduct-based" language in extradition treaties and ensure that cyber offences are expressly covered in future treaties and protocols.
- *Invest in capacity building.* Train police, prosecutors and judges in digital forensics, cross-border evidence handling and international cooperation.

IX. CONCLUSION

Cybercrime challenges the foundations of territorial criminal jurisdiction, yet it does not render the traditional principles obsolete. The objective territorial principle, the protective principle and, to a limited degree, the nationality and passive personality principles continue to furnish legitimate bases for extending criminal law beyond borders. The difficulty lies in managing concurrent claims and in converting legal authority into actual enforcement.

India has in sections 1(2) and 75 of the IT Act and section 1 of the BNS enacted expansive prescriptive provisions that are consistent with international law. But the effectiveness of that reach is limited by procedural ambiguity, dependence on slow channels of international assistance, a rigid locus-of-computer test and the absence of a principled approach to global orders. The path forward lies not in further widening of legislative reach, but in sharpening it through targeting-based nexus tests, building a robust framework for cross-border evidence and investing in international cooperation anchored in mutual respect for sovereignty and human rights. Only such a calibrated approach can reconcile the borderless nature of cyber offences with the territorial structure of the international legal order.

BIBLIOGRAPHY

Statutes and Rules

Bharatiya Nagarik Suraksha Sanhita 2023 (India)

Bharatiya Nyaya Sanhita 2023 (India)

Bharatiya Sakshya Adhiniyam 2023 (India)

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

Code of Criminal Procedure 1973 (India) (repealed)

Computer Fraud and Abuse Act, 18 USC s 1030 (United States)

Computer Misuse Act 1990 (United Kingdom)

Digital Personal Data Protection Act 2023 (India)

Extradition Act 1962 (India)

Indian Evidence Act 1872 (India) (repealed)

Indian Penal Code 1860 (India) (repealed)

Information Technology Act 2000 (India), as amended in 2008

Ministry of Electronics and Information Technology, CERT-In Directions under s 70B(6) of the Information Technology Act 2000 (28 April 2022)

Cases

Ajay Agarwal v Union of India (1993) 3 SCC 609

Anvar P V v P K Basheer (2014) 10 SCC 473

Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1

Banyan Tree Holding (P) Ltd v A Murali Krishna Reddy (2010) 42 PTC 361 (Del) (DB)

Dow Jones & Co Inc v Gutnick (2002) 210 CLR 575 (HCA)

Google Inc v Equustek Solutions Inc 2017 SCC 34 (Canada)

Google LLC v CNIL (Case C-507/17) ECLI:EU:C:2019:772

Google Spain SL v AEPD (Case C-131/12) ECLI:EU:C:2014:317

Glawischnig-Piesczek v Facebook Ireland Ltd (Case C-18/18) ECLI:EU:C:2019:821

Microsoft Corp v United States 829 F 3d 197 (2d Cir 2016)

Mobarik Ali Ahmed v State of Bombay AIR 1957 SC 857

R v Governor of Brixton Prison, ex p Levin [1997] AC 741 (HL)

Sharat Babu Digumarti v Government of NCT of Delhi (2017) 2 SCC 18

Shreya Singhal v Union of India (2015) 5 SCC 1

State of Maharashtra v Dr Praful B Desai (2003) 4 SCC 601

Swami Ramdev v Facebook Inc (Delhi HC, 23 October 2019)

The Case of the S.S. Lotus (France v Turkey) (1927) PCIJ Series A No 10

United States v Aluminum Co of America 148 F 2d 416 (2d Cir 1945)

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

Yahoo! Inc v La Ligue Contre Le Racisme et L'Antisemitisme 433 F 3d 1199 (9th Cir 2006) (en banc)

International Instruments

Convention on Cybercrime (Budapest, 23 November 2001) ETS No 185

Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence (12 May 2022) CETS No 224

United Nations Convention against Cybercrime, UNGA Res 79/243 (24 December 2024)

Harvard Research in International Law, Draft Convention on Jurisdiction with Respect to Crime (1935) 29 AJIL Supp 435

Books and Articles

Brenner S W, *Cybercrime: Criminal Threats from Cyberspace* (Praeger 2010)

Clough J, *Principles of Cybercrime* (2nd edn, Cambridge University Press 2015)

Daskal J, "The Un-Territoriality of Data" (2015) 125 Yale LJ 326

Goldsmith J and Wu T, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006)

Kohl U, *Jurisdiction and the Internet* (Cambridge University Press 2007)

Koops B-J and Goodwin M, "Cyberspace, the Cloud, and Cross-Border Criminal Investigation" (Tilburg Institute for Law, Technology and Society 2014)

Ryngaert C, *Jurisdiction in International Law* (2nd edn, Oxford University Press 2015)

Schmitt M N (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017)

Svantesson D J B, *Solving the Internet Jurisdiction Puzzle* (Oxford University Press 2017)

WHITE BLACK
LEGAL