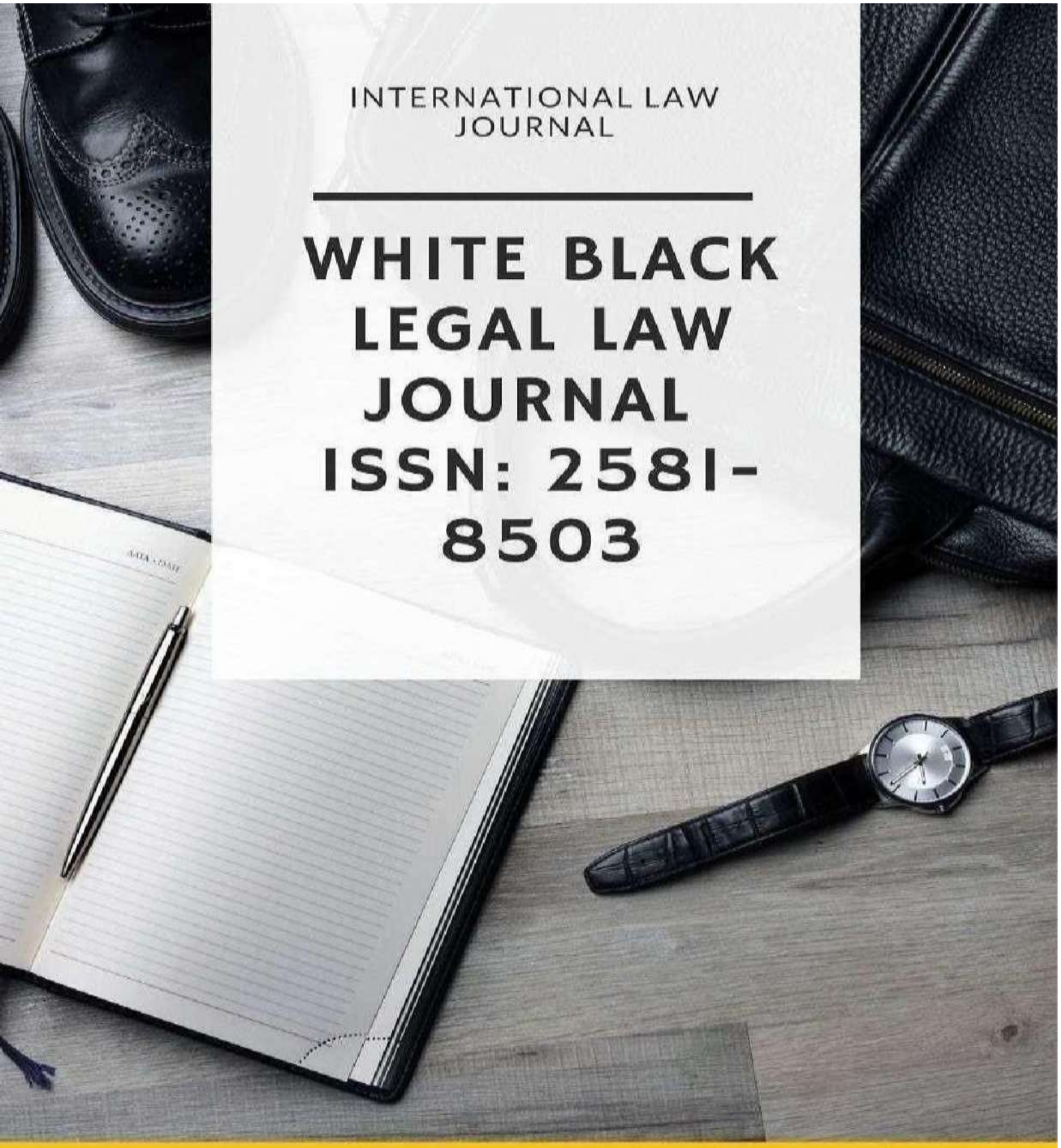

INTERNATIONAL LAW JOURNAL

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

www.whiteblacklegal.co.in
Volume 3 Issue 1 | June 2025 ISSN: 2581-8503

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | June 2025 ISSN: 2581-8503

RETHINKING TERRITORIAL JURISDICTION IN THE ERA OF DIGITAL BORDERS: A LOOK AT CARTOGRAPHIES OF CRIME

AUTHORED BY - ANUSHKA PATIL

Introduction: Deconstructing Borders in a Digitally Fluid World

Territorial jurisdiction, long seen as the axis around which criminal law revolves, is under severe strain. In a world where acts travel at the speed of light, traditional geographic boundaries, which were formerly critical in defining a state's ability to regulate and adjudicate, are rapidly becoming porous. The digital revolution has reshaped human interaction, enabling activities with global consequences to originate in one part of the world and have legal repercussions elsewhere.

India, a nation with an expanding digital presence and a rising reliance on cyberspace, is facing a legal dilemma. The country's criminal justice system, rooted in the Indian Penal Code (IPC) established during the colonial era, struggles to balance its territorial structure with the deterrent nature of digital crimes. This article's main concern is: how can the intangible be addressed by a jurisdictional framework based on the tangible?

In order to assess the nature of digital contacts, this paper suggests a conceptual shift from geography-based jurisdiction to a hybrid model that considers victim-centric impacts, relational closeness, and infrastructure control in addition to physical presence.

The Traditional Interpretation of Criminal Law Jurisdiction

A state's sovereign capacity to pursue crimes that take place within its borders is the fundamental tenet of criminal law. Section 1(3) of Bhartiya Nyaya Sanita, 2023 (BNS), which states that anyone can be punished for crimes committed in India, embodies this idea. [1] Section 1(5) of BNS, 2023 gives it jurisdiction over extra-territorial crimes carried out by Indian nationals and/or on Indian registered aircraft or ships.[2]

The Blackstonian view that law is inherently territorial is reflected in this concept. The state's geographical sovereignty was underlined by William Blackstone, who also emphasized that no

foreign state could impose laws outside of its borders. This strategy was appropriate for a time when crime was constrained by geographical boundaries.

Nonetheless, expectations like the universality principle (piracy, for example) continued to allude to a more adaptable legal imagination even in the 19th century. We must use this imagination even more in the 21st century.

Cyberspace: A Threat to National Boundaries

The sphere of cyberspace has no boundaries. A criminal in Romania, a server in the USA, a victim in Delhi, and a financial intermediary in Singapore could all be involved in an email, tweet, or hack. As a result, the conventional approach to identifying the crime scene falls apart.

Section 66 of the Information Technology Act,2000, defines hacking as any dishonest or fraudulent act defined in Section 43, such as unauthorized access, data tampering, or damage to computer systems, with the aim to inflict unjust loss or harm.[3] Section 78 of BNS,2023, penalizes cyberstalking and harassment, while Section 356 of BNS,2023, addresses defamation. Importantly, Section 66F of the IT Act,2000 defines cyberterrorism as acts committed with the intent to threaten India's unity, integrity, security, or sovereignty, or to instil fear in the public, by gaining unauthorized access to computer resources and disrupting or harming critical infrastructure. The victim and perpetrator may live in different countries that the server hosting the content.

It has been difficult for judicial decisions to change. A French court ordered Yahoo! to block French users' access to Nazi artifacts in Yahoo! Inc. v. LICRA (2001). However, U.S. courts refused to execute the decision, citing First Amendment safeguards.[4] The Delhi High Court ordered the removal of defamatory content worldwide in Swami Ramdev v. Facebook Inc. (2023),[5] indicating an assumption of jurisdiction based on impact rather than origin. In a similar vein, the Delhi High Court ruled in Banyan Tree Holding v. A. Murali Krishna Reddy (2010) that jurisdiction might be established by 'purposeful availment' of Indian markets via an interactive website.[6]

These cases highlight how the effects doctrine is increasingly being used to establish cyber jurisdiction.

The Indian Legal System and Its Limitations

India's principal law to combat cybercrimes is the Information Technology Act, 2000. According to Section 75, which allows for extraterritorial application, the Act covers any crime committed outside of India as long as it involves a computer that is situated in India.[7]

However, in the era of cloud computing and decentralized systems, this server-centric approach becomes problematic. Digital presence and virtual domicile are not defined by law. Additionally, there is little enforcement of such prohibitions, particularly when offenders operate out of nations with inadequate structures for mutual legal aid.

In Shreya Sinhgal v. Union of India (2015) [8], Section 66A, which penalized offensive electronic messages, was overturned because it was ambiguous and infringed upon Article 19(1)(a) of the Indian Constitution. Although the ruling was progressive, it also demonstrated how unaccustomed the judiciary is to the subtleties of digital technology.

Comparative Perspective: The International Digital Jurisdiction Experiments

The minimum contacts criterion from International Shoe Co. v. Washington (1945) is used in the US.[9] This has developed into the Zippo Sliding Scale test in cyber law, which determines jurisdiction according to how interactive a website is.[10] This method has been critiqued, meanwhile, as being out of date and insufficient for capturing the relational dynamics of online behaviour.

By claiming jurisdiction over organizations that handle the data of EU individuals, regardless of their location, the General Data Protection Regulation (GDPR) of the European Union represents a substantial shift. In effect, GDPR 2(2) shifts the focus of jurisdiction from actors or servers to subjects.[11]

Companies that handle Chinese data are subject to extensive extraterritorial duties and are required to localize their data under China's Cybersecurity Law (2017).[12] This is an example of data nationalism, which asserts control over infrastructure to assert digital sovereignty.

A Functional Theory of Jurisdiction in Progress

It is important to develop a functional theory of jurisdiction, because a purely geographical approach has limitations. A four-part model is proposed: the actor's intent, the victim's or impact's location, the infrastructure (such as servers or ISPs), and the type of harm (economic, reputational, or psychological).

For example, if a ransomware attack originates from a foreign country and targets Indian hospitals, the infrastructure involved is in India, the victims are Indian, and the consequences are significant. The assertion of jurisdiction by Indian courts is justified by the intent to harm Indian interests as well as the physical impact within Indian territory.

International Gridlock and Enforcement

Enforcement is still a significant obstacle even in cases where jurisdiction is claimed. Mutual Legal Assistance Treaties (MLATs), on which India depends, are frequently cumbersome and slow.[13] Evidence retrieval may take months, during which time data may be encrypted or deleted.

Concerns over sovereignty and unequal representation throughout the writing process are the main reasons India does not sign the Budapest Convention on Cybercrime.[14] However, by avoiding some diplomatic obstacles, the Second Additional Protocol (2022) permits more direct collaboration with private businesses.[15] India's capacity to enforce cybercrime laws might be significantly improved by joining this convention.

Human Rights and Constitutional Implications

It is crucial to protect fundamental rights when extending jurisdiction, the Supreme Court ruled in Justice K.S. Puttawamy v. Union of India (2017)[16] that, in accordance with Article 21, privacy is essential to life and liberty. As a result, jurisdictional rules ought to be written to prevent sweeping data acquisition or overzealous surveillance.

Despite not being officially codified yet, the Delhi and Madras High Courts have acknowledged the right to be forgotten in their rulings. Particularly in the digital age, when information is permanent and available everywhere, the idea aims to strike a balance between the public interest, press freedom, and human dignity.

Rethinking Digital Jurisdiction: Legal and Policy Suggestions

To align India's legal system with digital realities, several steps are necessary. First, definitions of cloud-based infrastructure and virtual presence must be added to the IT Act. Second, to enable faster international cooperation, India should consider ratifying the Budapest Convention and its supplementary protocol. Third, judges need training in digital evidence handling, blockchain, and cyber forensics. Fourth, establishing a sovereign data regulator is essential to monitor cross-border data flows and assert jurisdiction. Fifth, a digital ombudsman could be created to handle user complaints and multinational cyber concerns. Public-private collaborations with companies like Meta, Google, and Twitter can build trust in digital governance and improve compliance with court rulings.

Conclusion: Cross-Border Jurisdiction

Topography does not apply to the digital world. The crime scene of the 21st century is a network rather than a physical location. A code-based world cannot be governed by land-based laws. A jurisprudence that transcends location without sacrificing sovereignty is urgently needed.

A hybrid jurisdictional paradigm that takes into account the relational, functional, and impact-based logic of cyberspace has been argued for in this book. This kind of change is epistemological rather than just administrative. It demands that the law give up its geographical narrow-mindedness and adopt an ontological change in the way that injury, presence, and power are understood.

In a world without borders, justice can only then continue to have meaning.

Footnotes

1. Bhartiya Nyaya Sanhita, 2023, Section 1(3).
2. Bhartiya Nyaya Sanhita, 2023, Section 1(5).
3. Information Technology Act, 2000, Section 66.
4. Yahoo! Inc. v. LICRA, 169 F. Supp. 2d 1181 (N.D. Cal. 2001).
5. Swami Ramdev v. Facebook Inc., CS(OS) 27/2019, Delhi HC.
6. Banyan Tree Holding (P) Limited v. A. Murali Krishna Reddy & Anr., 2010 SSC OnLine Del 3780.
7. Information Technology Act, 2000, Section 75
8. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
9. International Shoe Co. v. Washington, 326 U.S 310 (1945).
10. Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997)

11. GDPR, Regulation (EU) 2016/679, Article 3(2).
12. Cybersecurity Law of the People's Republic of China, 2017.
13. Ministry of Home Affairs, Government of India, Mutual Legal Assistance Treaties (MLATs)
14. Council of Europe, Convention on Cybercrime (Budapest Convention), ETS No. 185, 2001.
15. Council of Europe, Second Additional Protocol to the Convention on Cybercrime, CETS No. 224, adopted 2022
16. Justice K.S. Puttawamy (Retd.) v. Union of India, (2017) 10 SSC 1.