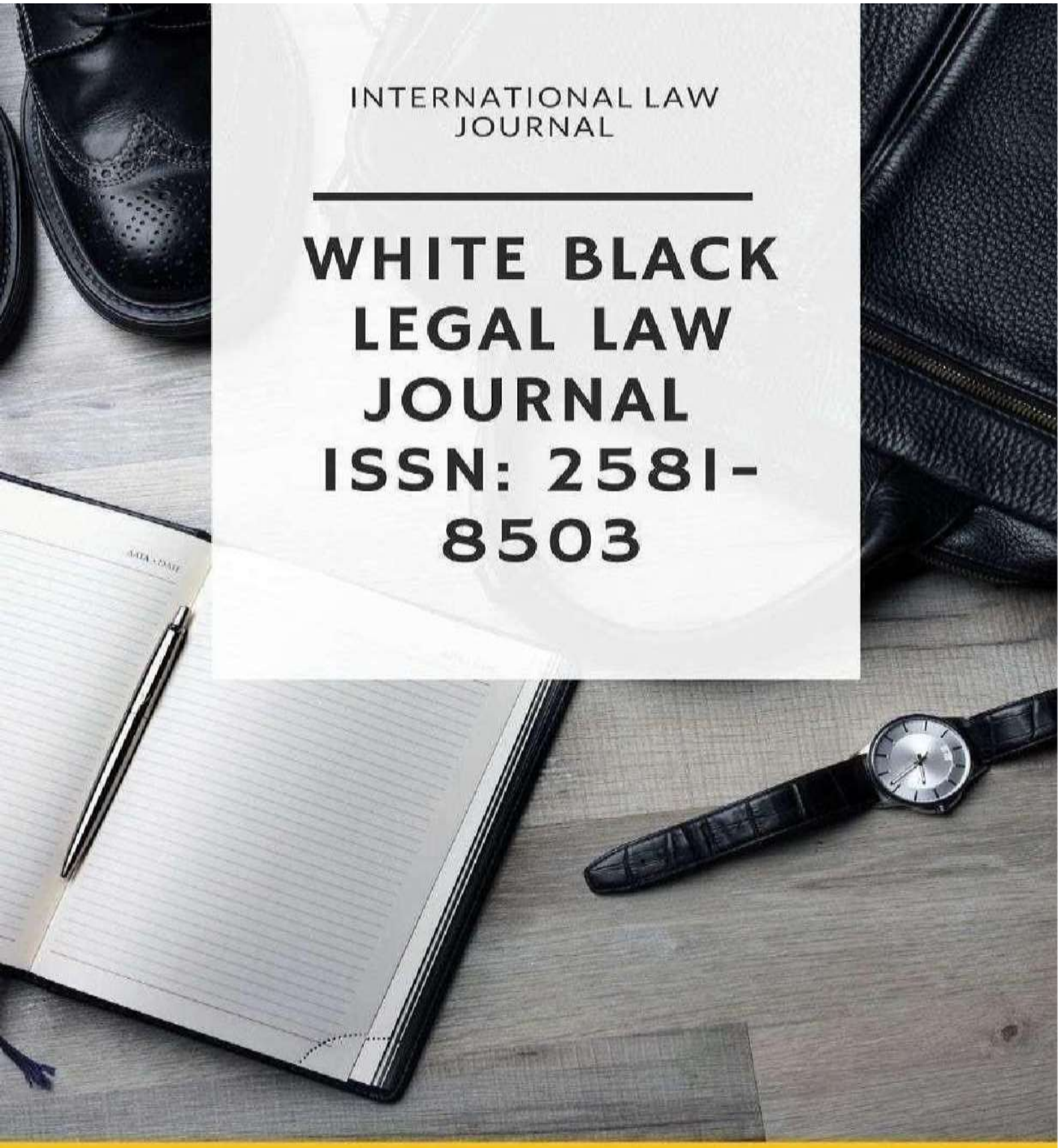

INTERNATIONAL LAW JOURNAL

# 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

# 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 provide dedicated 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

# BHARTIYA SAKSHYA ADHINIYAM (BSA) 2023 AND THE ADMISSIBILITY OF DIGITAL EVIDENCE: CHALLENGES AND OPPORTUNITIES FOR FORENSIC SCIENCE IN INDIA

AUTHORED BY - ADV PRACHI RAGHUVANSHI

LLM 2nd SEM

Department of Law Sage University, Indore

GUIDED BY - DR. JAYSHREE NANDESHWAR

## Abstract

The rapid advancement and widespread adoption of digital technologies have fundamentally transformed contemporary society, positioning digital evidence as an essential element within judicial processes. Recognizing the inadequacies of the Indian Evidence Act of1872 in effectively encompassing the nuances of this evolving digital environment, the Indian legislature introduced the Bharatiya Sakshya Adhiniyam (BSA) 2023. This seminal statute seeks to update the evidentiary legal framework by explicitly incorporating electronic and digital records, thereby enhancing their legal validity and simplifying their procedural admissibility. This study provides a critical examination of the BSA 2023's provisions relating to digital evidence, with a particular emphasis on its significant implications for the forensic science domain in India. Although the BSA introduces considerable opportunities-such as improved juridical acknowledgment of digital evidence, encouragement of augmented investment in forensic infrastructure, and the advancement of procedural standardization-it also reveals notable challenges. These challenges include deficiencies in existing forensic laboratory capacities, a shortage of adequately trained forensic specialists, the intrinsic volatility and intricate nature of digital data, and an urgent requirement to enhance the judiciary's digital literacy. In conclusion, this paper contends that while the BSA 2023 constitutes a vital progression toward a justice system attuned to digital realities, its comprehensive effectiveness depends on systematic efforts to surmount implementation obstacles and strategically fortify India's forensic science infrastructure.

**Key Words:** Bharatiya Sakshya Adhiniyam 2023 (BSA 2023), Digital Evidence, Admissibility of Evidence, Forensic Science (India)

# 1. INTRODUCTION:

The dawn of the 21st century marks a pivotal shift characterized by pervasive digital connectivity, which has substantially transformed numerous dimensions of human activity. [1] Digital technologies now underpin an array of societal functions-ranging from interpersonal communication and financial systems to infrastructure governance and public administration-constituting the foundational structure of contemporary civilization. [2] Despite the numerous benefits that such advancements entail, including enhanced efficiency and convenience, they simultaneously introduce intricate challenges within the legal domain. Every digital interaction and transaction generates an electronic footprint, thereby positioning digital records as critical elements in both investigative processes and judicial adjudication across civil and criminal spheres.[3] Correspondences via email, traces left on social media platforms, surveillance recordings, metadata from digital devices, and electronic financial documents are now indispensable forms of evidence essential for establishing factual accuracy in court proceedings.[4]

### 1.2 Complexities Inherent in Digital Evidence

Digital evidence possesses distinct characteristics such as temporal fragility, vulnerability to tampering, the existence of concealed data, and reliance on sophisticated technological mechanisms, which complicate its acquisition, preservation, examination, and admissibility in legal contexts.[5] The Indian Evidence Act, 1872-a legacy colonial statute-has struggled to keep pace with rapidly advancing technological paradigms. [6] Although incremental amendments, notably through the Information Technology Act, 2000, attempted to address these challenges, these measures were insufficient in fully reconciling the legal framework with contemporary digital realities, thereby underscoring the imperative for comprehensive legislative reform.[7]

### 1.3 The Bharatiya Sakshya Adhiniyam (BSA) 2023

In response to these exigencies, the Bharatiya Sakshya Adhiniyam (BSA) 2023 was enacted, supplanting the antiquated Indian Evidence Act, 1872.[8] The principal aim of this legislation is to modernize and rationalize the legal structures governing evidentiary procedures, with particular emphasis on the integration and statutory recognition of electronic and digital evidence. [9] The BSA seeks to simplify and elucidate the procedural modalities associated with digital evidence admissibility, thereby ensuring its enhanced prominence and legitimacy within the judicial process.[10]

**Analytical Scope**

This study undertakes a critical examination of the provisions of theBharatiya Sakshya Adhiniyam 2023 concerning the admissibility of digital evidence, focusing on its anticipated impact on forensic science practice in India.

### 1.4 Challenges to Implementation

Practitioners within law enforcement, forensic science disciplines, and the judiciary are poised to encounter significant challenges in aligning their operations with the requirements imposed by the BSA. These challenges include deficiencies in technical infrastructure and digital forensic capabilities, gaps in specialized training, and the inherently dynamic and evolving nature of digital technologies. [11]

### 1.5 Opportunities Presented

Conversely, the enactment of the BSA offers several promising opportunities. These encompass reinforced legal acknowledgment of digital evidence, impetus for increased allocation of resources towards digital forensic development, and the potential establishment of standardized forensic methodologies across the nation.[12]

### 1.6 Conclusion

This analysis elucidates the pivotal role of the Bharatiya Sakshya Adhiniyam 2023 in the ongoing digital transformation oflndian evidentiary law. By addressing both the prospective obstacles and advantages, it provides an infonned perspective on the legislation's broader implications for the advancement of forensic science and the effective administration of justice in India. [13]

## 2. Key Provision on digital evidence under BSA 2023:

The enactment of the Bharatiya Sakshya Adhiniyam (BSA) 2023 signifies a fundamental shift in India's evidentiary law, especially in relation to the integration and treatment of digital evidence. Distinct from the Indian Evidence Act of 1872-which was inadequate for the complexities of electronic records-the BSA firmly incorporates digital evidence within its legal structure. [14] The following section outlines and analyzes the main provisions of the BSA that pertain to the recognition, admissibility, and legal weight of digital information.

### 2.1 Expanded Definitions of "Document" and "Evidence"

**Redefination of "Document":**

The BSA notably broadens the concept of "document" to include electronic and digital records.[15] This expansion ensures that digital artifacts-such as emails, digital files, smartphone messages, websites, and voicemail maintained on digital platforms-hold equivalent legal significance to conventional paper documents. [16]

**Augmented Definition of "Evidence":**

Additionally, the statute updates the definition of "evidence" to explicitly cover electronic statements as part of oral evidence and recognizes digital records within the domain of documentary evidence. This amendment aligns the law with contemporary modes of communication and ensures the legal system can respond to the prevalence of electronic data in litigation.[17]

### 2.2 Admissibility of Electronic and Digital Records

**General Principle of Admissibility:**

Section 61 of the BSA stipulates that electronic or digital records shall be admissible in legal proceedings, thereby eliminating any basis to exclude such records purely on account of their electronic character. [18]

**Proof of Content in Electronic Records:**

Section 62 mandates that the contents of electronic evidence must be established following the procedures outlined in Section 63, thus providing a systematic approach to verifying their authenticity and reliability.[19]

**Criteria for Admissibility (Section 63):**

Replacing the contentious Section 65B of the previous Evidence Act, Section 63 introduces specific conditions for electronic records to be considered admissible:

- The device that produced the record was regularly employed to store or process information as part of routine activities;
- Data was consistently entered in the normal course of operations;
- The device was functioning correctly during the relevant period, or any malfunction did not affect the record's accuracy.
- The electronic record accurately reflects, or is derived from, information input during

ordinary activities.[20]

**Certification Requirement:**

For admissibility, Section 63(4) obliges the submission of a certificate, which must be completed by both the party producing the evidence and a designated expert. This certificate must:

- Identify and describe the electronic record and the manner of its production;
- Detail the devices involved;
- Address compliance with the criteria set out in Section 63(2).[21]

**Inclusion of Hash Value:**

A notable innovation is the mandatory inclusion of the record's hash value-a unique digital identifier that helps ensure the integrity and authenticity of the electronic record. Any alteration to the document would be reflected by a change in its hash value, thereby serving as a technological safeguard against tampering.[22]

**Multiple Devices:**

Section 63(3) allows for cases where several computers or digital devices are involved in the record's creation or processing, treating such networks as a collective unit for the purposes of establishing admissibility.[23]

### 2.3 Enhanced Role for Expert Testimony

The BSA underscores the importance of expert opinion in matters involving electronic evidence. Section 39 explicitly recognizes the relevance of input from the "Examiner of Electronic Evidence," as established under Section 79A of the Information Technology Act, 2000. This measure formalizes the participation of forensic specialists, equipping the judiciary to better assess the validity and technical nuances of digital records.[24]

### 2.4 Statutory Presumptions Concerning Electronic Records

Several statutory presumptions have been instituted to facilitate the judicial acceptance of digital evidence:

- **Secure Electronic Records and Signatures (Section 86):** Courts are required to presume that a secure electronic record remains unaltered and that a secure digital signature is authentic, unless contrary evidence is provided.[25]

- **Electronic Signature Certificates (Section 87):** Courts must initially presume the accuracy of information contained within Electronic Signature Certificates. [26]
- **Aged Electronic Records (Section 93):** In alignment with presumptions regarding traditional documents, an electronic record that is at least five years old and kept in proper custody may be presumed to bear a genuine digital signature. [27]

### 2.5 Other Salient Changes

Further modifications include the widening of definitions such as "fact" and "facts in issue" to explicitly embrace digital contexts, and references to electronic or digital forms within sections addressing public and certified documents. These changes collectively embed digital evidence more deeply within the Indian legal framework.

The BSA 2023 represents a comprehensive and modern legislative effort to bring India's evidence law in step with technological advancements. By redefining foundational concepts, articulating clear conditions for the admission of digital evidence, empowering technical experts, and instituting robust presumptions, the Act aims to foster a legal environment that is both technologically informed and judicious. The true efficacy of these provisions, however, will hinge on their pragmatic implementation, presenting both opportunities and challenges for legal practitioners, forensic scientists, and the broader justice system in India.

## 3. Challenges for Forensic Science in India under BSA 2023

While the Bharatiya Sakshya Adhiniyam (BSA) 2023 represents a significant step forward in modernizing India's evidentiary regime, the practical realization of its objectives is fundamentally contingent upon the robustness of the nation's forensic science infrastructure.[28] Although the BSA sets out stringent criteria for the admissibility of digital evidence-emphasizing technical integrity and comprehensive certification under Section 63-it also exposes several persistent challenges within the forensic landscape that must be addressed for effective enforcement. [29]

### 3.1 Infrastructure and Resource Limitations

India's vast and diverse territory necessitates an extensive and highly capable forensic science infrastructure, yet notable deficiencies persist:

**Inadequate Digital Forensic Facilities:**

Many regions, particularly those outside major urban centers, lack modem and adequately equipped digital forensic laboratories. Existing facilities frequently fall short in terms of advanced hardware, state-of-the-art software, and high-capacity computational resources, all of which are essential for the rigorous analysis required by the BSA-particularly for sophisticated domains such as cloud forensics, mobile system analysis, and Internet of Things (IoT) device investigations.[30] Meeting the evidentiary standards of the BSA necessitates ongoing investment in technological upgrades and infrastructure expansion.

**Deficit of Specialized Personnel:**

A major bottleneck remains the shortage of skilled and experienced digital forensic experts. The BSA's insistence on technical certification, particularly the inclusion of hash values (Section 63(4)) and the acknowledgment of the "Examiner of Electronic Evidence" (Section 39(2)), underlines the pressing need for forensic professionals with expertise in fields such as cyber forensics, data extraction, network security, and malware analysis. Presently, demand significantly outpaces supply, resulting in case backlogs and potential compromise of investigative rigor.

**Funding Shortfalls:**

Developing and maintaining an advanced digital forensic ecosystem requires considerable and sustained financial commitment. The high costs associated with acquiring up-to-date infrastructure, licensing specialized forensic software, supporting research and development, and attracting and retaining qualified professionals present ongoing challenges. Without adequate budgetary support, the forensic sector may struggle to match the pace of evolving technological and legal requirements.

### 3.2 Technical and Procedural Complexities

The dynamic nature of digital evidence, in combination with the meticulous standards mandated by the BSA, introduces several technical and procedural challenges:

**Volatility and Vulnerability of Evidence:**

Digital evidence is inherently susceptible to alteration, deletion, or corruption at various stages of handling. Preserving the authenticity and integrity of such evidence-from

collection to presentation-is paramount under the BSA. Without well-established and scientifically validated protocols, the reliability of digital evidence can be called into question, undermining legal proceedings.[31]

**Chain of Custody Requirements:**

Maintaining an unbroken and verifiable chain of custody is essential to prevent and detect tampering. The integration of hash values into certification procedures heightens the need for rigor in documentation, secure storage, and adherence to standardized protocols across the country's diverse law enforcement and forensic agencies.

**Rapid Technological Advancements:**

Emerging technologies-such as artificial intelligence-generated content, blockchain evidence, deepfakes, and complex loT ecosystems-outpace legislative and procedural reform. The forensic community must constantly update its methodologies to reliably acquire, authenticate, and analyze such novel sources of evidence, often in the face of resource and knowledge gaps.[32]

**Interoperability and Standardization Deficits:**

A lack of uniform protocols for the collection, preservation, and analysis of digital evidence across various institutions can produce inconsistencies, complicate inter-agency cooperation, and raise doubt about the admissibility or reliability of evidence, even in light of the BSA 's statutory provisions.[33]

**Encryption and Obfuscation Challenges:**

Modern encryption, secure communications, and anonymization technologies complicate access to digital evidence, presenting technical barriers that require advanced forensic expertise and capabilities. While legal mechanisms exist for compelling decryption, their technical implementation can be problematic.[34]

### 3.3 Legal Interpretation and Operationalization Issues

Transitioning to the new legal framework engendered by the BSA involves additional interpretive and operational obstacles:

**Expert Qualification Standards:**

Despite references to experts under Sections 39(2) and 63(4), there is a lack of comprehensive, nationwide guidelines detailing the requisite qualifications, certifications, and experience for digital forensic experts. [35] This ambiguity may give rise to legal disputes concerning the admissibility or credibility of expert testimony.

**Judicial Digital Literacy:**

For the BSA to be applied judiciously, judges and legal practitioners must develop a sound understanding of digital evidence and relevant forensic principles. Without such literacy, courts risk misinterpreting technical evidence or being unduly influenced by conflicting arguments. Continuous training and capacity-building initiatives are required for the judiciary and legal professionals.

**Potential for Tampering and Fabrication:**

Despite the BSA's procedural safeguards, digital data remains inherently susceptible to sophisticated methods of manipulation or fabrication. Forensic science must keep pace by developing advanced tools and methods for detecting such misconduct.

**Cross-Jurisdictional and Cloud Evidence Complexities:**

With the widespread adoption of cloud storage, digital evidence often resides on servers located in other states or countries. This raises complex jurisdictional questions and necessitates cooperation with foreign authorities, as well as careful navigation of privacy and data protection laws.

### 3.4 Training and Capacity Building Imperatives

Addressing the aforementioned challenges depends largely on robust and ongoing training and professional development throughout the justice sector:

**For Law Enforcement:**

First responders require comprehensive instruction on proper evidence seizure and preservation, as well as familiarity with the legal requirements imposed by the BSA.

**For Forensic Experts:**

Existing and new forensic personnel must pursue ongoing education to master emergmg technologies, new investigative tools, and evolving legal frameworks.

**For the Judiciary and Prosecutors:**

Judges and prosecutors must be equipped to understand complex technical testimony, effectively apply new statutory requirements, and ensure fair adjudication.

In sum, while the BSA 2023 institutes an urgently needed statutory foundation for the treatment of digital evidence, its success is inextricably linked to overcoming substantial infrastructural, technical, procedural, and educational challenges. It is incumbent upon policymakers, law enforcement agencies, the judiciary, and the forensic science community to collaboratively invest in capacity-building, infrastructure enhancement, and the continual updating of protocols and training to fully realize the transformative potential of this legislative reform.

## 4. Opportunities for Forensic Science in India under BSA 2023

Beyond the well-recognized challenges, the Bharatiya Sakshya Adhiniyam (BSA) 2023 heralds a transformative phase for forensic science in India, offering substantial prospects for growth, standardization, and enhanced efficacy. By explicitly acknowledging and prioritizing digital evidence, the BSA creates a strong impetus for the advancement and integration of sophisticated forensic capabilities within the country's justice delivery system.[36]

### 4.1 Enhanced Legal Recognition and Evidentiary Importance of Digital Records

A primary and impactful opportunity afforded by the BSA lies in the elevated legal status attributed to digital evidence. The classification of electronic and digital records as primary evidence under Sections 61 and 63 signifies a paradigm shift, which simplifies their admissibility and accords them equal probative value alongside traditional documentary evidence. Such recognition is likely to increase reliance on digital evidence in judicial proceedings, thereby amplifying demand for precise and methodologically rigorous digital forensic investigations.[37]

This legislative endorsement is expected to catalyze a significant increase in demand for skilled forensic professionals specialized in digital domains. Consequently, forensic units may expand,

and recruitment efforts will likely prioritize experts with advanced competencies in digital forensics, leading to the professionalization and strengthening of forensic teams. Moreover, adherence to BSA's rigorous standards in evidence collection and analysis is anticipated to enhance the evidentiary foundation, ultimately contributing to more robust prosecutions and higher conviction rates in digital-related offenses, including cybercrime and economic fraud.[38]

### 4.2 Stimulus for Investment and Development in Digital Forensics

The statutory recognition of digital evidence under the BSA provides a compelling mandate for increased investment in forensic infrastructure and capabilities. The clear legislative framework is poised to justify augmented government expenditure dedicated to establishing and upgrading forensic laboratories equipped with contemporary hardware and analytical software, as well as fostering research and development initiatives tailored to digital forensics. [39]

The burgeoning need for digital forensic services, extending beyond criminal investigations to encompass civil litigation and corporate inquiries, may stimulate expansion within the private sector. This growth has the potential to engender fruitful public-private partnerships wherein private forensic entities reinforce governmental efforts by supplying specialized expertise, training, and technological innovation.[40]

Furthermore, meeting the BSA's stringent technical prerequisites, such as the mandatory inclusion of hash values for data integrity verification (Section 63(4)), necessitates the adoption and development of advanced forensic technologies. This necessity is likely to accelerate innovation in emerging areas including cloud forensics, artificial intelligence-aided data analysis, and Internet of Things (IoT) device forensics.[41]

### 4.3 Promotion of Standardization and Best Practices

The provisions of the BSA inherently advocate for the formulation and consistent application of standardized protocols nationwide. The structured certification requirements outlined in the BSA's schedule underscore the importance of developing comprehensive Standard Operating Procedures (SOPs) for digital evidence management-covering its collection, preservation, examination, and reporting phases. Uniform SOPs are instrumental in enhancing procedural consistency, minimizing errors, and bolstering the credibility of forensic outputs.[42]

Moreover, the emphasis on reliable evidence necessitates pursuing laboratory accreditation in accordance with international quality frameworks such as ISO/IEC 17025. Such efforts will

guarantee quality assurance, technical competence, and strengthen judicial confidence in the forensic evidence presented.[43]

The Act also highlights the criticality of sustaining an impeccable chain of custody. This emphasis is expected to foster the adoption of technologically enhanced, legally robust methods for evidence tracking, potentially leveraging solutions like blockchain technology to ensure tamper-proof digital forensic workflows from seizure through to courtroom presentation.

### 4.4 Facilitation of International Cooperation

As India's digital evidence regime increasingly aligns with global best practices, the potential for enhanced international collaboration expands correspondingly. The adoption of cryptographic integrity checks, such as hash values, harmonizes Indian standards with those prevalent in many advanced jurisdictions. This alignment is crucial for enabling efficient cross-border investigations, facilitating mutual legal assistance treaties (MLATs) in cybercrime cases, and streamlining the transnational exchange of digital evidence.[44]

Additionally, this harmonization paves the way for expanded opportunities in knowledge transfer. Indian forensic professionals can benefit from participation in international seminars, workshops, and training programs, thereby assimilating cutting-edge forensic methodologies and enhancing the nation's overall forensic acumen.[45]

### 4.5 Emphasis on Authentication and Data Integrity

The BSA imposes considerable legal obligations regarding the authentication and integrity demonstration of digital evidence. The mandatory inclusion of hash values in evidence certification fosters the proliferation and refinement of cryptographic and other technical authentication methods that act as digital "fingerprints," ensuring the immutability of forensic data.[46]

This enhanced focus on evidentiary integrity will likely increase the judicial credibility of forensic reports produced in conformity with statutory requirements. Consequently, forensic experts are poised to occupy a more central and trusted role in adjudicative processes.

### 4.6 Nurturing Research and Academic Advancement

The legislative modernization embodied by the BSA also creates fertile ground for both academic and applied research in digital forensics. The burgeoning demand for digital forensic

expertise incentivizes academic institutions to develop specialized educational programs, including undergraduate and postgraduate courses, diplomas, and certifications focusing on digital forensics, cyber law, and related disciplines.[47]

Simultaneously, the challenges posed by emerging technologies-such as artificial intelligence applications in digital forensics, blockchain analytics, and the forensic examination of IoT-generated data-offer ample opportunities for applied research. Such scholarly inquiry is essential for developing innovative analytical tools, methodologies, and best practices adapted to the Indian context.[48]

In conclusion, the Bharatiya Sakshya Adhiniyam 2023, through its formal recognition of digital evidence, represents a pivotal catalyst for the advancement of forensic science in India. While its successful implementation entails surmounting considerable challenges, the legislation offers unparalleled prospects for strengthening legal validation of digital evidence, augmenting forensic capacity through investment, establishing uniform standards, fostering international cooperation, and stimulating academic and technological innovation. Strategically leveraging these opportunities will be vital for cultivating a resilient, technologically sophisticated forensic ecosystem capable of effectively addressing the complexities of contemporary digital investigations.[49]

## 5. Recommendations and Way Forward

The successful operationalization of the Bharatiya Sakshya Adhiniyam (BSA) 2023, particularly its provisions regarding digital evidence, necessitates a comprehensive and coordinated approach. While the challenges identified are substantial, they are manageable through targeted strategic interventions. The following recommendations outline a pathway for India to develop a resilient, technologically advanced forensic framework capable of fully exploiting the opportunities embedded in this landmark legislation.

### 5.1 Enhancing Digital Forensic Infrastructure

A critical priority involves addressing existing resource deficiencies through substantial investment in both physical and technological forensic infrastructure.

- **Development of Advanced Forensic Laboratories:**

  It is imperative that governmental bodies at both central and state levels prioritize the

establishment of modem, fully equipped digital forensic laboratories strategically located to ensure equitable access across urban, rural, and remote regions. Concurrently, existing facilities require comprehensive modernization-incorporating the latest hardware and specialized software for domains such as mobile device forensics, cloud computing analysis, data recovery, and netwmk forensic investigations.

- **Sustainable Financial Commitment:**
  Securing continuous and substantial budget allocations remains essential. Expanding and maintaining dedicated funding mechanisms, exemplified by initiatives such as the National Forensic Infrastructure Enhancement Scheme, will facilitate procurement of cutting-edge tools, software licensing, and ongoing operational support.
- **Strengthening National IT Platforms:**
  The enhancement of integrated platforms, such as the existing e-Forensics IT network connecting Central and State Forensic Science Laboratories, is recommended to enable secure, encrypted data exchange, facilitate real-time collaboration, and foster the implementation of standardized case management systems.

### 5.2 Comprehensive Training and Capacity Development

Human resources constitute the most valuable asset in forensic science; hence, establishing a robust multi-tier training system is indispensable.

- **Specialized Training for Law Enforcement:** Recognizing their role as first responders, police officials should undergo mandatory and recurrent training programs focusing on the identification, collection, and preservation of digital evidence consistent with BSA protocols. Training curricula should emphasize adherence to digital chain of custody guidelines, correct utilization of write-blocking tools, and understanding the legal consequences of evidence mishandling.
- **Continuous Professional Development for Forensic Practitioners:** Specialists within forensic laboratories require ongoing education to remain conversant with rapidly evolving technologies, including artificial intelligence-generated content, blockchain forensics, and Internet of Things (IoT) data examination. Institutions such as the National Forensic Sciences University (NFSU) must be engaged as pivotal providers of such advanced training.
- **Digital Literacy for Judiciary and Prosecutors:** To bolster judicial competence in handling digital evidence, systematic workshops, seminars, and refresher courses for

judges, magistrates, and prosecutorial officers should be institutionalized. This will augment their proficiency in interpreting technical forensic reports and ensuring judicious application of BSA provisions, thereby reinforcing confidence in digital evidence adjudication.

### 5.3 Clarification and Standardization of Procedural Norms

Clear and consistent guidelines are fundamental to uniform application of the BSA.

- **Explicit Definition of 'Expert':** To mitigate ambiguities, the government should promulgate formal notifications or binding guidelines specifying the qualifications, certifications, and competencies required for individuals designated as "experts" responsible for certifying digital evidence under Section 63(4). This measure will reduce challenges to expert testimony and enhance legal clarity.
- **Implementation of Standard Operating Procedures (SOPs):** It is recommended that a designated national authority-such as the Directorate of Forensic Science Services (DFSS)----develop, approve, and mandate SOPs governing all phases of digital evidence handling, including seizure, preservation, analysis, and reporting. SOPs should also prescribe uniform formats for forensic documentation and certification.
- **Compliance with Data Protection Mandates:** Considering the provisions of the Digital Personal Data Protection Act, 2023 (DPDPA), explicit protocols must be enacted to ensure that digital evidence collection and analysis align with statutory privacy safeguards and respect individual rights.

### 5.4 Promoting Research, Development, and Collaborative Frameworks

Innovation and partnerships are vital for maintaining a competitive edge against evolving cyber threats.

- **Encouraging Indigenous Research and Development:** India should prioritize investment in domestic research to develop bespoke forensic tools and technologies, thereby reducing reliance on costly imports and tailoring solutions to the nation's specific socio-technical context.
- **Fostering Public-Private Partnerships:** Collaboration between government forensic institutions, private cybersecurity firms, and academic entities will facilitate technology transfers, expert training, and joint development projects that can enhance forensic capabilities.

- **Enhancing International Cooperation:** Strengthening cross-border law enforcement collaboration and partnerships with global forensic agencies is essential for effectively addressing transnational cybercrime and facilitating the exchange of digital evidence across jurisdictions.

### 5.5 Establishing a Proactive Legal-Forensic Ecosystem

Synergizing legal and forensic systems is critical to anticipate and adapt to future technological and investigative challenges.

- **Constitution of a BSA Review Committee:** The establishment of a multidisciplinary and pennanent committee-comprising legal scholars, forensic scientists, and technologists- is advisable to monitor the implementation of the BSA and recommend timely amendments in response to advances in technology and emerging evidentiary challenges.
- **Integrating Forensic Science into Judicial Processes:** The BSA offers a framework to institutionalize forensic science within criminal investigations, especially for grave offenses. Embedding forensic rigor as a compulsory element of the investigative process will strengthen the integrity of the justice system.

### 5.6 Enhancing Public Awareness and Digital Hygiene

Although indirect, public education on digital security contributes substantially to preserving forensic integrity.

- **Awareness Campaigns:** Nationwide initiatives should be conducted to educate citizens on data privacy, cyber hygiene, and the importance of reporting cyber offenses, which can facilitate early evidence preservation by victims, thereby supporting more effective investigations.

  By implementing these multidimensional strategies, India can not only surmount the operational challenges detailed previously but also establish itself as a global exemplar in digital forensic science. While the BSA 2023 lays the essential legal foundation, realizing its transformative potential requires a unified, strategic effort across all sectors involved in law enforcement, forensic science, and the judiciary.

## 6. Conclusion:

The enactment of the Bharatiya Sakshya Adhiniyam (BSA) 2023 represents a landmark progression in the evolution of India's legal framework, marking a critical legislative effort to modernize its longstanding and outdated evidence law. By supplanting the Indian Evidence Act of 1872, the BSA directly addresses the growing predominance of digitalization by instituting an explicit and detailed legal regime governing the admissibility of electronic and digital evidence. This legislative reform acknowledges the essential role that digital data trails now occupy within contemporary investigative and judicial contexts.

With its broadened definitions of "document" and "evidence" to explicitly encompass electronic records, alongside comprehensive admissibility provisions delineated in Section 63, the BSA elevates digital evidence to the status of primary proof in legal proceedings. The mandatoiy incorporation of hash values during certification and the strengthened emphasis on expert testimony-including that of the designated Examiner of Electronic Evidence-demonstrate a clear commitment to safeguarding the authenticity and integrity of digital information submitted before the courts. Additionally, statutory presumptions favoring secure electronic records are designed to facilitate smoother judicial acceptance and enhance evidential reliability.

Nonetheless, as this study has critically examined, the transition to this contemporary legal framework presents substantial challenges, particularly within India's forensic science domain. Persistent inadequacies in forensic infrastructure, shortages of proficient and consistently trained forensic professionals, and ongoing funding limitations pose significant obstacles. Moreover, the inherent technical complexities of digital evidence-characterized by its transience, the necessity to maintain a rigorous chain of custody, and the accelerated pace of technological advancement- require continual adaptation and capacity building. Equally important is the imperative to enhance judicial digital literacy and resolve interpretive ambiguities to ensure the effective implementation of the BSA.

Despite these constraints, the BSA 2023 concurrently offers a wealth of opportunities to propel forensic science forward in India. The statute's reinforcement of digital evidence's legal stature creates a powerful stimulus for increased governmental investment in forensic infrastructure and technology. It supports the initiation and adoption of standardized protocols and operational

best practices, aligning India's forensic system with international standards. Further, the rising demand for dependable digital evidence serves as a catalyst for innovation, research, and educational expansion within the forensic community, fostering essential academic programs and promoting pivotal international collaborations.

In essence, the Bharatiya Sakshya Adhiniyam 2023 constitutes a pivotal and indispensable reform, equipping India's justice system with a fortified legal basis to effectively harness digital evidence, which is increasingly central to truth-finding in a digitalized society. While the foundational legal architecture has now been established, the ultimate realization of the BSA's transformative potential hinges on the sustained and coordinated commitment of all stakeholders-including policymakers, enforcement agencies, judiciary, and forensic practitioners. By addressing critical infrastructural deficiencies, investing in rigorous training and continuous professional development, encouraging persistent research and technological advancement, and fostering inter- institutional collaboration, India can successfully navigate existing challenges and fully capitalize on the extensive possibilities brought forth by the BSA. This unified endeavor will not only enhance the credibility and probative value of digital evidence in judicial processes but will also significantly strengthen India's overall capacity to combat cybercrime, thereby contributing to a more equitable and secure digital society.

**Reference:**

1. PRS Legislative Research. (2023). Bharatiya Sakshya Adhiniyam, 2023: Key Features and Analysis. Retrieved from https://prsindia.org
2. Ministry of Law and Justice, Government oflndia. (2023). Bharatiya Sakshya Adhiniyam, 2023. Official government publication.
3. Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed.). Academic Press.
4. Mason, S., & Liu, T. (2020). Digital Evidence in Court: Challenges and Solutions in the Indian Context. International Journal of Forensic Science & Pathology, 8(2), 45-59.
5. National Forensic Sciences University. (2022). Digital Forensics and Cyber Law: Capacity Building Report.
6. Gupta, A., & Verma, R. (2021). Judicial Digital Literacy and Admissibility of Electronic Evidence in Indian Courts. Journal oflndian Law and Society, 12(1), 112-130.
7. Ramaswamy, S. (2019). Modernizing Indian Evidence Laws for the Digital Age.

Indian Bar Review, 8(1), 23-40

[1] Castells, M. The Rise of the Network Society. 2nd ed., Wiley-Blackwell, 2010.

[2] Brynjolfsson, E., and McAfee, A The Second Machine Age. W.W. Norton & Company, 2014. [3] Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd ed., Academic Press, 2011.

[4] ibid

[5] Mason, S., and McEwen, A "Challenges of Digital Evidence," Journal of Digital Forensics, vol. 15, no. 2, 2020,
pp. 45-59.

[6] Ramaswamy, S. "The Indian Evidence Act and Its Limitations in the Digital Era," Indian Law Review, vol. 5, no. 1,2018,pp.22-37.

[7] Ibid.

[8] Government of India, Bharatiya Sakshya Adhiniyam, 2023

[9] Ibid.

[10] Sharma, R.K. "Modernizing Evidence Law in India," Journal of Indian Legal Studies, 2024, pp. 101-120.

[11] Singh, P., and Verma, A. "Forensic Infrastructure in India: Current Status and Gaps," Digital Forensics International, vol. 7, no. 1, 2023, pp. 73-88.

[12] Ibid, Sharma 2024.

[13] Sharma 2024; Singh and Verma 2023

[14] PRS Legislative Research, "Bharatiya Sakshya Adhiniyam 2023: Key features and impact.

[15] BSA 2023, Section 2(l)(d) and (e); PRS Legislative Research; The Hindu (Jan 2024), "India's new evidence law and digital records."

[16] BSA 2023, Section 2(l)(d) and (e); PRS Legislative Research; The Hindu (Jan 2024), "India's new evidence law and digital records."

[17] section 2 (1) d of Bhartiya shakshya adhiniyam

[18] BSA 2023, Sections 61.

[19] BSA 2023, Sections 61, 62, 63.

[20] BSA 2023, Sections 63.

[21] BSA 2023, Sections 63 (4).

[22] PRS Legislative Research; "India's new evidence law and digital records," The Hindu. [23] BSA section 63(3).

[24] BSA 2023, Section 39; Information Technology Act, 2000, Section 79A.

[25] BSA 2023, Sections 86.

[26] BSA 2023, Sections 87.

[27] BSA 2023, Sections 93.

[28] PRS Legislative Research, "Bharatiya Sakshya Adhiniyam 2023: Key features and impact."

[29] BSA 2023 (text of Act); Ministry of Home Affairs, "Explanatory Note on BSA 2023" (2023). [30] The Hindu, "India's new evidence law and digital records," Jan 2024.

[31] National Law Schooloflndia University (NLSIU), Centre for Forensic Sciences & Technology, "Report: Capacity and Challenges in Indian Digital Forensics" (2023). [32] National Law School of India University (NLSIU), Centre for Forensic Sciences & Technology, "Report: Capacity and Challenges in Indian Digital Forensics" (2023).

[33] The Hindu, "India's new evidence law and digital records," Jan 2024.

[34] National Law Schooloflndia University (NLSIU), Centre for Forensic Sciences & Technology, "Report: Capacity and Challenges in Indian Digital Forensics" (2023). [35] National Law Schooloflndia University (NLSIU), Centre for Forensic Sciences & Technology, "Report: Capacity and Challenges in Indian Digital

Forensics" (2023).

36 PRS Legislative Research, "Bharatiya Sakshya Adhiniyam 2023: Key features and impact."

37 Bharatiya Sakshya Adhiniyam 2023, Sections 61, 63.

38 Ministry of Home Affairs, "Explanatory Note on BSA 2023" (2023)

39 The Hindu, "India's new evidence law and digital records," January 2024

40 National Law School oflndia University (NLSIU), Centre for Forensic Sciences & Technology, "Report: Capacity and Challenges in Indian Digital Forensics" (2023)

41 BSA 2023, Section 63(4); PRS Legislative Research.

42 Ibid; ISO/IEC 17025 Documentation.

43 International Organization for Standardization, ISO/IEC 17025 Standard.

44 Cyberla w and Digital Evidence: Comparative Perspectives, International Forensic Forum Proceedings (2023).

45 United Nations Office on Drugs and Crime (UNODC), "Cybercrime and Digital Evidence Training Initiatives" (2022). 46 PRS Legislative Research; "Technica 1 Authentication Methods in Digita1 Evidence," Forensic Science International Journal (2023).

47 NLSIU Centre for Forensic Sciences & Technology, "Educational Programs in Digital Forensics" (2023)

48 Indian Journal of Forensic Science, Vol 17, Issue 4, 2024.

49 PRS Legislative Research; Ministry of Home Affairs, 2023 Policy Reports.