https://doi.org/10.69974/glslawjournal.v8i2.214

GLS Law Journal, Vol. 08, Issue 02; July - December 2026

Admissibility of Digital Evidence under Bhartiya Shakhya Adhiniyam, 2023: Balancing Data Privacy and Challenges in Light of the DPDP Act, 2023

Dr Trisha Mittal[1]

Abstract

The introduction of new criminal laws has introduced overarching changes in the criminal justice system. The Bhartiya Sakshya Adhiniyam, 2023 includes electronic records as documents and lays down the procedure for proving its admissibility under section 63. However, there remain gaping loopholes in its operation, especially since proving the authenticity of digital records has been a matter of judicial debate recently. The Digital Personal Data Protection Act, 2023, designed to protect data privacy of individuals, prescribes strict accords for handling, storing, recording and transmission of data. This article aims to identify the points of conflict between the two legislations and suggests measures that can be employed to arrive at a harmonious resolve. The objectives sought to be achieved by these contemporary laws is making adequate usage of modern technology in administration of justice and protection of data privacy of individuals, while public welfare remains the end goal.

Keywords: Digital Evidence, Right to Privacy, Data Protection, Bhartiya Sakshya Adhiniyam, 2023, Digital Forensics

Introduction

The Law on Evidence is the most significant procedural law governing legal systems, both civil and criminal, which makes it application widely universal. The term "evidence" is borrowed from the Latin word "*evidens or evidere"* meaning to "show clearly; to make clear to the sight; to discover clearly; to make plainly certain; to ascertain; to prove."[2] Due to its significance, there is an inherent need for it to remain fixed, yet adapt gradually to changing times. Owing to these reasons, the Indian Parliament recently introduced an overhaul in Indian criminal laws, in a bid to decolonize them.[3]

The **Bharatiya Sakshya Adhiniyam, 2023** is one of the legislations (*hereinafter* referred to as the "Adhiniyam" or "BSA, 2023") that replaced the English-made **Indian Evidence Act, 1872** (*hereinafter* referred to as the "Act" or the "IEA, 1872"). The Adhiniyam introduces new provisions pertaining to the digital evidence and electronic records which were earlier not present in the Act. Admission of electronic records as digital evidence has been put to test before Indian courts and given a pass considering the evolving nature of technology in all aspects of human life. The law cannot remain a mere spectator to advancements in technology. The introduction of digital electronic records in an endeavor to widen terms as a part of "documents" under **section 2(d) and sections 61 and 63 of the BSA, 2023** are a culminated effect of the same thought. The law seeks to achieve the modern goal of making digital and computer-generated records easily admissible in court.

---

[1] Assistant Professor of Law, Maharashtra National Law University, Nagpur.

[2] Sarkar law of evidence: In India, Pakistan, Bangladesh, Burma, Ceylon, Malaysia & Singapore, (2016).

[3] Ministry of Home Affairs *available at*: https://www.mha.gov.in/en/commoncontent/new-criminal-laws (last visited October 10, 2024).

The law on data privacy is another aspect that is roped in when we speak of digital records. The law on data privacy in India is in nascent stages and is ready to be propelled into action by the **Digital Personal Data Protection Act, 2023**[4] (*hereinafter* referred to as the "DPDP Act,2023")**.** The Apex Court recognized the right to privacy of citizens as an intrinsic part of right to life and liberty in the landmark ***Puttaswamy judgement***[5] which paved the path for data privacy laws. The DPDP Act, 2023 is supposed to entwine the scattered provisions for data protection under the **Information Technology Act, 2000** (*hereinafter* referred to as the "IT Act, 2000") and the **IT (Sensitive Personal Data or Information) Rules, 2011** (*hereinafter* referred to as "IT Rules, 2011"). The objective of the DPDP Act is to allow individuals to protect their personal data while also permitting its processing for lawful purposes. The Act harbors provisions for protection of personal data and liability for breach of data privacy.

The simultaneous enforcement of the two laws may result in a consequential overlap, giving rise to questions such as standards that need to be followed for collecting personal data that may be admitted as evidence before the court and whether such data may even be considered reliable. The law must be balanced to protect constitutionally vested rights and duties of law enforcement agencies.

The Law on Digital Evidence: Bharatiya Sakshya Adhiniyam, 2023

The BSA, 2023 has introduced remarkable changes in evidence law by incorporating provisions for digital and electronic records. Earlier, the unmentioned and unspecified part of evidence, that of electronic documents, was included in the procedure through judicial interpretation and amendments to the original Acts. Enormous scrutiny and deliberation were attributed to digital evidence before it could be made legally admissible in the court of law due to concerns of tampering, breach of privacy and overall credibility of such evidence. However, the need for recognizing digital evidence was felt ever so starkly in the age of impending digitization.

Law prior to 2023

The IEA, 1872 contained special provisions for producing electronic records before the court and standards for proving their authenticity. **Section 65A of IEA, 1972** stated that an electronic record may be submitted as evidence if it satisfied the criteria under **section 65B of IEA, 1872,**[6] which further states that evidence may be generated as a computer output and stored in any medium, in printed or digital forms, and can be produced as evidence before the court. There are conditions which must be satisfied before such evidence is made admissible before the court, such as the information must be produced by a computer which was "regularly in use during the period",[7] the information must have been routinely entered into the computer while it was operated ordinarily and,[8]and regularly throughout the said period, and any information that the output is derived from was being fed into it continuously.[9] All of this, becomes admissible after being attested by an individual occupying

[4] Times of India *available at:* https://timesofindia.indiatimes.com/india/digital-personal-data-protection-bill-now-an-act-receives-presidents-assent/articleshow/102674040.cms (last visited October 11, 2024).
[5] K.S Puttaswamy v. Union of India, (2017) 10 SCC 1.
[6] Indian Evidence Act, 1872 (Act 1 of 1872), s. 65A.
[7] *Id.*
[8] *Id.*
[9] *Id.*

an official position with respect to the device from which the information was obtained, or any other person responsible for managing the device.

The Act mandates the furnishing of a certificate as per **section 65-B** for producing an electronic record in the manner prescribed. It states the particulars of the electronic record or prescribes any of the matters under **section 65-B (2).** The certificate acts as a mode of proof for admitting evidence from computer output where original records cannot be produced.[10] The two provisions operated as the legal lynchpins for governing the admissibility of electronic evidence in a legal proceeding.[11]

Judicial pronouncements

The Indian judiciary has debated and concluded its stance on electronic evidence through a catena of judgements. The most recent ruling of the court in ***Arjun Panditrao Khotkar*** in which the court accepted the necessary admissibility of electronic evidence, supplemented by a certificate from a person having official authority over the device.[12] The previous views have been similar in the sense that the court fosters greater ease to the admissibility of electronic record in a bid to promote access to digital records and modern communications, which is greatly dependent upon technology. Previously, in ***Shafi Mohammad v. State of H.P,*** the Apex Court encouraged the admissibility of electronic evidence in the lack of an expert certificate under **section 65B (4),** giving an outlet to the possibility that not every person might have access to the original device from the electronically stored information was obtained.[13] Though, concerns about the absence of accountability rise in the lack of such a certificate, the eagerness of the courts to carve out an exception in that regard show a zeal toward admissibility of electronic evidence.

Even in the case of ***Arjun Panditrao Khotkar,*** the court accepts that there may be peculiar instances when a crucial piece of evidence may be deemed admissible under rules for admissibility of relevant secondary evidence under **section 64 and 65 of the IEA, 1872** even if not strictly complying with the procedure for admissibility under **section 65B(4).**[14] The continuing trend proves that the law relating to admissibility of digital evidence may be further relaxed in the future to make electronic records easily admissible. No deemed fiction needs to be employed to imagine the fallacies that may emerge out of such a proposition for unrestricted admissibility of electronic information produced by persons other than the actual owners of electronic devices, without their permission.

Such concerns were noted by the court in case of ***Anvar P.V.*** where it remarked that the requirement of certificate cannot be substituted by any other forms of evidence that may hint at the authenticity of the evidence.[15] The provisions for electronic record deemed admissible as primary evidence under the BSA, 2023 runs contract to the holding in this judgement since there is no such criteria mandated for evidence being produced as primary evidence.

Present Law

The Bharatiya Sakshya Adhiniyam, 2023 has taken a forward step toward embracing technological change by introducing a number of provisions in the legislation. The change is

[10] Sonu v. State of Haryana (2017) 8 SCC 570.
[11] Anvar P.V v. P.K Basheer, (2014) 10 SCC 473.
[12] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
[13] Shafi Mohammad v. State of H.P, (2018) 2 SCC 801.
[14] Supra note 10.
[15] Supra Note 11.

welcome for keeping the Indian legal landscape abreast with contemporary developments. The definition of "documents" under **section 2(d)** was enlarged to specifically include "electronic and digital records",[16] which would include emails, server logs, documents on devices, laptops, smartphones, websites, locations, voice mails, etc.[17] The term "evidence" now includes statements made electronically within the ambit of oral evidence and all documents presented as digital or electronic record as documentary evidence.[18]

The trilogy of **section 61, 62 and 63 of the BSA, 2023** form the framework for digital evidence under the Indian evidence law. **Section 61** states that no information can be refused from being admitted on the ground that it is digital or electronic in nature.[19] This lays down the governing principle of general admissibility of digital evidence in a legal proceeding, that nothing hinders the production of an evidence which is digital or electronic.[20]

Although, the admissibility of digital evidence is not rendered unconditional. It is followed by **section 62** which lays down that electronic records submitted as evidence may be proved as per the conditions given in **section 63.**[21] The latter section is a replica of the older law under section 65B which provides necessary conditions for admissibility of a record generated from a computer output i.e., the regular operation of the system in ordinary course of activities where similar kind of data is fed into and generated from the system.[22] The **Adhiniyam** also provides for a certificate signed by the person in charge of maintaining or operating the device and an expert before it can be considered for admissibility under this section.[23]

The requirement of a certificate by the person in-charge of the device reflects concerns about the genuineness and authenticity of such electronic records, and why the necessity of a certificate cannot be totally dispensed with it.[24] Moreover, the **Adhiniyam** now provides a standard form for the certificate under its schedule which was not present in the older law.[25] The standardization of the process further implies its necessity and mandatory nature for dealing with all forms of electronic records.

The **Adhiniyam** clarifies the scope of documents admissible as "primary evidence" under **section 57** and adds four more explanation to include digital records. The provision states that primary evidence would include each copy of an electronic record created or stored simultaneously or sequentially, any such record produced from proper custody, any video recording which is transferred to another device, each of its stored recordings and each copy of digital record stored automatically in a computer would be considered primary evidence.

---

[16] BSA 2023 s. 2(1)(d).
[17] A.F Moussa, A.F. Electronic evidence and its authenticity in forensic evidence, 11 Egypt J Forensic Science 20 (2021).
[18] Supra note 15
[19] BSA 2023 S.61
[20] PRS India *available at:* https://prsindia.org/billtrack/the-bharatiya-nyaya-second-sanhita-2023 (last visited on October 14, 2024).
[21] BSA 2023 s.62.
[22] BSA 2023 s. 63(1).
[23] Id.
[24] *Chhtrapati, D., Chaudhari, S. P., Mevada, D., Bhatt, A., & Trivedi, D. (2021). Research Productivity and Network Visualization on Digital Evidence: A Bibliometric Study. Science & Technology Libraries, 1–15.* https://doi.org/10.1080/0194262x.2021.1948486
[25] Id.

Following a line of judicial interpretation, such evidence would not need supplementation by a certificate under **section 64(4)(c),** since such a requirement is primarily applicable to secondary evidence.[26] Therefore, electronic records are now directly admissible as primary evidence under the **BSA, 2023.**

The Law on Data Protection: The DPDP Act, 2023

Backdrop of the Act

India's proposed law on data protection is the **Digital Personal Data Protection Act, 2023** which is aimed at governing the storage and collection of personal information.[27] The Act, not in effect as of yet, is aimed to be made applicable to user information collected online, or collected offline and later converted into digital form.[28] The Act will apply to processing of data beyond the Indian territory where the Data Principals are receiving goods or services from organizations not within the territory of India.[29] The objective of the Act, as stated by the Parliament, is to ensure the right of citizens to guard their personal data and allow the necessary processing of data for legitimate purposes. The need for promoting data integrity arose right after the judgement in ***Puttaswamy,***[30] so did the need for processing data in all modern transactions. This part of data sphere could be guarded only be regulating such processing of personal data and imposing strict liability on organizations carrying out such processing. This is something the Act seeks to achieve.

Provisions and Principles

The Act creates a prominent pathway for instilling a strict data privacy regime by introducing regulations and relevant terminology such as "data principal" which means any individual whose personal data is concerned[31] and "data fiduciary" meaning any person who decides the means and methods of using the data obtained.[32]

The Act is governed by the principles of "purpose limitation" and "collection limitation", borrowed from the principles of Data Protection that govern the European GDPR.[33] **Purpose limitation** which implies that the data collected must be utilized for the specified purpose only and which consent has been obtained and **Collection Limitation** which is construed to mean that only such personal information is collected that is necessary for processing for a specified purpose.[34] Thus, consent forms a crucial aspect in the framework for data protection.

Breach of Data and Rights of Data Principal

As per the Act, any information, which renders a person identifiable, counts as personal data as per **section 2(t)**[35] and any unauthorized use of processing of such data, without the

---

[26] Supra Note 9.
[27] Khilansha Mukhija and Shreyas Jaiswal, "Personal Data Protection Act, 2023 in light of European Union's GDPR" 4.1 *JCLJ* 654 (2023).
[28] DPDPA, 2023 (Act 22 of 2023), s. 3(a).
[29] Id.
[30] Supra note 4
[31] DPDPA, 2023 (Act 22 of 2023), s. 2(j).
[32] Id.
[33] GDRP, Art. 5.
[34] Kermina Minoo Patel, The 2023 Digital Personal Data Protection Act: Evaluating its strength in protecting citizens data, 4.1 *JCLJ* 454 (2023).
[35] Supra note 29.

permission of the person to whom it belongs, any acquisition, use, storage, collection of the personal data that comprises its integrity, confidentiality or availability amounts to a breach of such data.[36]

The Act also prescribes rights of data principal that can be exercised with regards to such a processing.[37] Broadly, the rights of the data principal include: -

- **The right to seek information**: The data principal may seek information about the personal data being processed by the data fiduciary; information relating to any summary of personal data, or any information about such data being shared with other data fiduciaries.[38]
- **The right to correct and erase personal data**: The data principal can at any time request for modification or erasure of personal data, with respect to which consent had been obtained previously. The data fiduciary is bound to correct or erase any information relating to such data upon receiving such request.[39]
- **The right to grievance redressal:** The data principal is granted the right of redressal for grievances caused to them by the actions of data fiduciary or consent manager in the course of processing of their personal data.[40]
- **The right to nominate:** The data principal can also choose another person to exercise their rights with respect to the processing of their personal data in instances like death.[41]

Liabilities and Breach of Data Privacy

Prior to the DPDP Act, 2023, the provisions of data privacy were governed by the framework under the **IT (Amendment) Act, 2008 and the IT (SPDI) Rules, 2011.** The breach of privacy is explained within the 2000 Act in the terms that anyone who has obtained access to any material information, in the course of discharging duties under a lawful contract, and discloses such information to another person knowing that such disclosure will cause wrongful gain or wrongful loss, commits a breach of confidentiality and data privacy.[42][43]

The present Act will repeal the provision for compensation under **section 43A of the IT Act** which states that anybody corporate that deals with personal information of an individual and is negligent in the handling of such information,[44] would be liable to pay compensation.[45] The DPDP Act, 2023 introduces its own provision for liability in case of any breach of privacy committed in the course of data processing.[46] The liability is in the form of monetary penalty that could range up to Rs. 250 crores where a data fiduciary fails to

[36] Id.
[37] Id.
[38] Id.
[39] Id.
[40] Id.
[41] Id.
[42] The Information Technology Act, 2000 (Act. 21 of 2000), s. 72A.
[43] Shiv Shankar Singh, "Privacy and Data Protection in India: Critical Assessment" 53 *Journal of the Indian Law Institute* 663-677 (2011).
[44] Malvika Jayaram, "The Business of Privacy: From Private Anxiety to Commercial Sense? A Broad Overview of Why Privacy Ough to Matter to Indian Businesses," 4 *NUJS L Rev* 597.
[45] IT Act 2000 s. 43A.
[46] DPDPA 2023 (Act 22 of 2023), s. 33.

implement reasonable security safeguards to prevent breach,[47] to be decided on the basis of nature, gravity or duration of breach, nature of personal data, any gain or loss caused, etc.[48][49] There could be varying penalties for other breaches or violations of the Act rallying up to 50 crores. The hefty sum of penalty showcases the hard legislative intent to strictly monitor the data privacy regime.[50]

Apart from the monitory penalty, the Data Protection Board may also make a reference to the Central Government for blocking access to any information hosted, stored or transmitted by a data fiduciary, in case of repeated breaches of data privacy.[51] In larger public interest, that government may take stringent steps to protect the data integrity of data principals.

The Legal Conflicts between BSA, 2023 and DPDPA, 2023

The two acts necessarily scrimmage upon each other in their operation. The **BSA, 2023** is a marvelous attempt at overhauling India's evidence laws and instituting newer forms of law on a fulcrum of technology. New tools and channels of communications that have come into the picture after the advent of technology require acknowledgement in law for appropriate regulation. The objective of the **Adhiniyam** remains to decolonize the archaic law and foster means to make digital evidence more relevant and easily admissible before the court.[52]

The **DPDP Act, 2023,** on the other hand, is another revolutionary move toward building a data privacy regime that India was lacking till recently. The objective is blatantly stated as to ensure the protection of basic rights while allowing for necessary processing of data for legitimate purposes. Data protection is recognized as an extended arm of right to privacy, which itself is considered an extension of right to life and liberty under Article 21.[53] The Court recognized the need for a separate legislation for protecting data privacy of citizens even at the time of amendment to the IT Act in 2008. The Apex Court had held that disclosure of private documents belonging to a person without their consent would amount to breach of confidentiality.[54]

If you try to understand the immediate goals of both legislation, admissibility of digital evidence, in primary or secondary form, is sure to impinge upon the data privacy of individuals and eventually resulting in breach of right to privacy, since the **Adhiniyam** does not provide any measures or procedures for ensuring lawful retrieval of such information. The only reference made to lawful means of obtaining digital records is in **section 57 of the BSA, 2023** wherein explanation 5 provides that any electronic record presented from "proper custody" may be admitted as primary evidence, unless it is disputed.[55] However, instances in the new criminal laws such as **section 152 of BNS, 2023** that require electronic communications that 'instigate separatist' feelings[56] to be 'recorded, intercepted, detained' by service providers[57] even

[47] Lexology, *available at*: https://www.lexology.com/library/detail.aspx?g=1f7752ab-eb0a-467b-ac23-746c5888d29f (last visited on October 14, 2024).
[48] DPDPA 2023 (Act 22 of 2023), s. 33(2).
[49] Supra Note 32.
[50] Anirudh Burman, "Understanding India's New Data Protection Law" *Carniege Endowment for International Peace* (2023),
[51] DPDPA (Act 22 of 2023), s. 37(1).
[52] Malhotra, C., & Malhotra, U, "Putting Interests of Digital Nagriks First: Digital Personal Data Protection (DPDP) Act 2023 of India." *Indian Journal of Public Administration*, 70(3), 516-531 (2023).
[53] Supra Note 4.
[54] In District Registrar and Collector v. Canara Bank, AIR 2005 SC 186.
[55] BSA 2023 (Act 47 of 2023), s. 57, exp. 4.
[56] BNS, 2023 (Act 45 of 2023), s. 152.
[57] Telecommunications Acts, 2023.

if that results in infringing the end-to-end encryption of such communications, is a concerning disregard of data privacy rights.[58]

Right to Privacy: Not absolute

The right to privacy of citizens is undeniably granted protection through a combined framework of Art. 21 and its extensive interpretation by the Apex Court. As well as the privacy of citizens when it comes to protection of their data is the entire foundation behind the **DPDP Act of 2023.** However, the right to privacy safeguarded with stringent measures actually stands as an absolute right is a question that needs pondering.

The **DPDP Act, 2023 Act** itself provides its objective as an act that ensures the right of citizens to guard their personal information while at the same time ensuring the processing of data for all legitimate purposes. Now, a valid contention is made that processing of personal data for legal proceedings or any related matters, in furtherance of justice, is legitimate use of such data. The Act provides certain exemptions for processing of personal data by courts or tribunals for performance of regulatory and supervisory functions,[59] as well as for investigation or prosecution of any offence.[60] However, the concerns with regards to the modes and medium of attainment of such data is not totally disregarded.

The exemptions granted under the Act portray the subordinate nature of the right to privacy, in spite of its interpretation as a fundamental right under Article 21.[61] Right to privacy is tied with reasonable restrictions,[62] in the sense that any law that imposes reasonable restrictions upon it is held valid.[63] The right to privacy can be yielded to other rights that function for greater public interest, such as the right to information.[64] The reasoning behind such a subordinate operation is so that necessary function of the state may not be hindered by individual interest.[65] In a balance of individual interest against public interest, public interest takes primacy. At the same time, the court acknowledge such restrictions on right to privacy may only be established by a valid procedure and it must be just, fair, reasonable and non-arbitrary.[66]

Collection and production of evidence

The process of collection and production of digital evidence in the form of electronic records forms the crux of the current law on evidence. The procedure, means and medium of collection of electronic evidence holds significance for ensuring procedural fairness and the greater sanctity of law. Although, the right to privacy is considerably diluted when viewed through the lens of public interest, the privacy of individuals and confidentiality of their personal information could not be plainly violated in the name of state functions or necessary duties.[67]

---

[58] Rajesh Vellakkat, "Data Privacy Rights and Informed Consent" *PL (IT)* 80 (September, 2015).
[59] BSA, 2023 (Act 47 of 2023), s. 17(1)(b).
[60] Id.
[61] Aanandita Aneja, "Tracing the development of the Right to Privacy in India" 3.2 *JCLJ* 1350 (2023),
[62] Thalappalam Service Coop. Bank Ltd. v. State of Kerala, (2013) 16 SCC 82.
[63] Gobind v. State of M.P, (1975) 2 SCC 148.
[64] PUCL v. UOI, AIR 2003 SC 2363.
[65] Supra Note 59.
[66] State of Maharashtra v. Bharat Shanti Lal Shah, (2008) 13 SCC 5.
[67] Helen Nissenbaum, Protecting Privacy in an Information Age: The Problem of Privacy in Public, 17(5) *Law & Philosophy* 559 (1998),

The **Bharatiya Nyaya Suraksha Sanhita, 2023** allows for production of digital evidence collected during search and seizure by police officers under **section 185 of the Sanhita.** Such searches are to be recorded by the police officers on mobile phones.[68] The recording of such evidence on mobile phones, without specifying the procedure, storage, means of transmission may present another problem. Naturally, this would result in police officers recording such searches on their personal devices and storing them likewise. Currently, no provision exists within the law to prevent breach of confidentiality, alteration or tampering in such a scenario.[69]

Digital evidence, though proved to be standing on a progressive front, cannot be considered as thoroughly fruitful once their credibility is established through lawful means. This is the reason why the Judiciary is constantly pressing on the need to allow admissibility of electronic records with certification under **section 63(4).**[70][71] The court allowed an interception to be admissible, in spite of it not being recorded in strict conformity with law**.** ***Navjot Sandhu.*** The court also allowed the admissibility of digital evidence without the mandatory certificate requirement.[72]

However, this part of the ruling was overruled in ***P.K Basheer***[73] where the court once again established the mandatory nature of the certificate accompanying secondary electronic evidence. The court in its most recent ruling on digital ***Arjun Panditrao Khotkar*** has upheld the decision in ***Anvar,*** only applying occasional departure from the rule of producing a certificate under as per the law.[74]

Right to be forgotten

The collection of so much data poses a risk to right to privacy in a myriad ways, including the possibility of infinite storage of such data. Right to be forgotten is acknowledged as an intrinsic feature of right to privacy,[75] which entitles individuals to erasure of their personal data from unauthentic transmission or storage.[76] This simplifies the process of data collection by laying its foundation on consent.[77] Concerns had been raised on India's lack of strict data protection laws that would regulate the handling of such personal information,[78] which may also include biometric data of individuals.[79]

Digital evidence, and its handling by state authorities or other individuals, may impinge upon the fundamental right to have one's data regulated, deleted, or erased. Regulation of all forms of data collection is absolutely necessary to ensure personal integrity of citizens in the rising digital age.[80] The right to correction and erasure under the DPDP Act is a step to implement the right to be forgotten, which permits the data principal to completely erase their personal

[68] The Bhartiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023), s. 185(1).
[69] Bhartiya Sakshya Adhiniyam, 2023 (Act 47 of 2023) s. 57.
[70] Supra Note 10.
[71] N.S Nappinai, "Electronic Evidence- The Great Indian Quagmire" 3 *SCC J-41* (2019).
[72] State (NCT of Delhi) v. Navjot Sandhu (2005) 11 SCC 600.
[73] Supra note 10
[74] Supra Note 11.
[75] Supra Note 4.
[76] Google Spain SL, Google Inc. v. Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez, C-131/12.
[77] Michael L. Rustad, Sanna Kulveska, "Reconceptualizing the right to be forgotten to enable transatlantic data flow," 28 *Harv JL& Tech* 349 (2015).
[78] Abhinav Shrivastava, "Data Rights 2.0: Shifting Sands of Usage Rights in User-Data", 2.2 *JIPS* 54 (2019).
[79] Report of the Group of Experts on Privacy, Government of India (2012).
[80] Manupatra *available at*: https://articles.manupatra.com/article-details/Right-to-be-forgotten (last visited October 14. 2024).

information by withdrawing consent.[81] The GDPR harbors a similar provision for data protection.[82]

The collection of digital evidence for the purpose of production before court, laxation in statutory standards for production of such evidence, unauthorized surveillance and storage would all amount to breach of the right to be forgotten,[83] unless strict regulations and protocols are inculcated to prevent such mismanagement. The only provision that punishes such mishandling of data for negligent use and causing wrongful gain or loss is the IT (Amendment) Act, 2008.[84]

Why Digital Evidence is prone to challenges

The futuristic spurt toward forging a justice system built on digital evidence is impressive. Though any such revolutionary measure needs to be bolstered by additional regulations, procedures and protocols to ensure their proper implementation. Without a bulwark of supporting laws, any stringent overhaul of laws would fall flat. The system of digital evidence suffers from obvious limitations due to the same reason.

Breach of privacy: Placing restrictions on right to privacy in the course of furthering the duties of law enforcement, may severely encroach upon the fundamental rights of citizens.[85] Admissibility of illegally obtained evidence, procured digitally, through unethical means may experience a rise. The rule of procedural fairness has typically set the precedent that such evidence obtained through illegal means, or if there is involvement of the party submitting the evidence in any illegal conduct, such evidence automatically becomes inadmissible.[86] Earlier, the test for admitting an evidence was limited to its relevancy in the proceeding. This was the position beforee right to privacy was read into Article 21.[87]

At the present, the value of evidence illegally obtained or violative of constitutional right is diminished by judicial pronouncements. The doctrine of "fruits of poisonous trees" would find direct application.[88] The right of privacy itself is broadly interpreted, seeing that its scope is continuously expanded from a person, to personal property to personal data of an individual transferred to third party.[89] Any admissibility of controversially obtained evidence would have to be questioned by the courts on the degree of violations of rights and dignity in the process of obtaining and whether the circumstances justify the actions.[90] Any restriction by "established law," the new criminal laws in this case, will have satisfy a strict scrutiny of constitutional rights.

Chain of Custody: Proper chain of custody in digital evidence is crucial for the admissibility of evidence. Chain of custody needs to be maintained to ensure its integrity, which would essentially ensure its admissibility before the court.[91] Digital evidence, due to

[81] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 12(1).
[82] GDPR, art. 17.
[83] Tejashree J., "The need for the right to be forgotten in India", 5.1 *RFMLR* 106 (2018).
[84] IT Act (Amendment) Act, 2008 (Act 10 of 2009), s. 43A.
[85] Khushbu Jain, "The crossroads of Privacy and Digital Evidence" *The Sunday Guardian,* January 14, 2024.
[86] Caratube International Oil Co. LLP v. The Republic of Kazakhstan, ICSID Case No. ARB/13/13.
[87] Paras Marya, "A Relook at the admissibility of illegally or improperly obtained evidence" 8 *NLIU Law Review* 284 (2019).
[88] Talha Abdul Rahman, "Fruits of the Poisoned Tree: Should Illegally obtained evidence be admissible?" S-38 *PL May* (2011).
[89] Supra Note 26.
[90] Law Commission, *Evidence Obtained Illegally or Improperly*, (Law Com No 94, 1983) Ch.10A.
[91] Makhdoom Syed Muhammad Baqir; Saleem, Shahzad; and Zulqarnain, Roha (2017) "Protecting Digital Evidence Integrity and Preserving Chain of Custody," *Journal of Digital Forensics, Security and Law*: Vol. 12, Article 12.

its intangible nature, is prone to alternation and tampering and needs to be preserved with prescribed protocols to establish its authenticity.[92]

In the case of digital evidence, its credibility cannot be sufficiently determined by a certificate, much less if the discretion is left on the judges to decide its admissibility. The hash value of such electronic record along with that of the device from which it was procured need to be produced.[93] The stakes for proving the integrity of such evidence are thus high.

The chain of custody must remain unbroken and any possibility of tampering could reasonably result in the evidence being not admissible, even if it's inculpatory in nature.[94] The original digital evidence cannot be tampered with in any situation, which requires that utmost due diligence must be exercised while working with digital evidence.[95] The audit trail which forms a part of chain of custody must be meticulously maintained otherwise it would malign the entire findings of investigation.[96] With respect to chain of custody, the Apex Court has held from the moment of taking of a sample till the time investigation is closed, each person handling such evidence must be duly acknowledged to ensure that its integrity is uncompromised.[97]

Lack of adequate procedure: Lack of adequate procedure in recording, collection and storage of digital evidence and any presumption toward its reliability would foster the admissibility of inaccurate evidence.[98] On procedural aspect of evidence collection the Judiciary has been vocal about not permitting police officers to imperil the rights of individuals through illicit methods.[99] The **IT (Amendment) Act, 2008**[100] allowed for interception of electronic communication through mobile phones, emails, text messages etc., and a procedure through such interception was to be carried out is prescribed under **IT (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009.**[101] In the absence of any procedure which governs the standard of collection or recording of data, the possibility of abuse runs high.[102]

Even for the purpose of acquiring encrypted data or information to be produced as evidence, there is no procedure specified apart from the authority vested in the investigating authority to ask for such information.[103] Such wide and arbitrary powers, vesting in an official without meticulous rules for its regulation could potentially violate the right against self-incrimination of the accused.[104]

---

[92] Borquez P, Importance of chain of custody of evidences, *Europe PMC* (June 1, 2011).
[93] Devesh Banwani & Yatin Kalra, "Maintaining and Evaluating the Integrity of Digital Evidence in Chain of Custody" 10 *IJRTE* 90-96 (2021).
[94] Rahul v. State (NCT of Delhi), (2019) 20 SCC 196.
[95] Rohas Nagpal, "Cyber Crime & Digital Evidence-Indian Perspective," *Asian School of Cyber Laws* (2008).
[96] Swati Mehta, "Cyber Forensics and Admissibility of Digital Evidence," *PL* January S-23 (2012).
[97] Prakash Nishad v. State of Maharashtra, 2023 SCC Online SC 666.
[98] Supra Note 69.
[99] R.M. Malkani v. State of Maharashtra, (1973) 1 SCC 471.
[100] IT Act 2008 (Act 10 of 2009), s. 69.
[101] Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009.
[102] Lekshmi G.R., "Electronic Surveillance-A Tool for Invasion of Privacy," 32, 224, 224, (2008).
[103] BNSS 2023 s. 176(3), proviso
[104] Raveena Rai, "Challenges to Cyber Crime Investigation: A need for statutory and Infrastructural Reforms" 5 *CNLU LJ* 62 (2015).

Since the **BSA, 2023** lacks any explicit measures for regulating the procedure for storing, transmitting, or disposing of electronic records, which could make way for possible abuse and tampering of digital evidence.

Digital forensics: The **BNSS, 2023** now mandates forensic investigation and prescribes that the investigator must record the entire procedure in audio-video format.[105] In case of lack of forensic facilities, the facilities could be borrowed from neighboring states.[106] Further, **section 185 of the** of the **Sanhita** allows an investigating officer to conduct searches and a proviso within states that the search conducted needs to mandatorily recorded, preferably through a mobile phone.[107] This audio-video recording is sent to the Magistrate for taking cognizance of the offence.[108]

However, there is still a lack of experts, personnels, equipment, and infrastructure that needs to be acquired to give priority to the technology-centric provisions of the new laws.[109] Preservation and availability of digital forensic evidence needs to be ascertained since its improper handling can create significant investigative handicap.[110][111] The investigating officers, on the other hand, are reluctant in utilizing expert assistance and prefer dealing with forensics independently, which might result in misuse of discretionary powers or extraneous influence over the procedure of investigation.[112] The admissibility of such evidence improperly obtained is bound to be disallowed on the discretion of the judge.[113]

The Way Forward

The timely and proper implementation of the provisions under the **BSA, 2023** require extensive reforms. Both micro and macro changes must be introduced to allow a smooth overhaul of the justice system, since the current system is shaken by the impact of new laws. Suggestions can be made in the present diaspora that may lead the way in making the new laws appropriately functional.

The Apex Court has emphasized the need to formulate guidelines for collection of digital evidence, highlighting concerns about the absence of guidelines for seizure of electronic evidence.[114] Special note was made of the judgement given by the same court in ***K.S Puttaswamy,*** signifying that the era may be advancing toward data sharing and digital admissibility, but it only widens the scope of privacy and stretches it to cover data privacy of individuals. Similar guidelines are required under the Adhiniyam to ensure digital evidence before the court is admitted from 'proper custody', particularly now since the digital evidences can be admissible as primary evidence.[115]

The **BSA, 2023** ought to harbor a provision pertaining to the maintenance of chain of custody, since chain of custody is practically required to be established to avoid the possibility of

[105] The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023), s. 176(3).
[106] Supra Note 101,
[107] BNSS, 2023 (Act 46 of 2023), s. 185(1).
[108] Id.
[109] Drishti Jain& Vagisha Sagar, "Digital Forensics Tools for Social Media Investigations: Special Emphasis on User Privacy" 2.1 *DSNLUJ SCI Tech L* 43 (2022).
[110] Supra Note 83.
[111] Christopher L.T. Brown, "Computer Evidence, Collection & Preservation" *Charles River Media*, Hingham MA (2006).
[112] Dr. G.K. Goswami, "Spreading Wings of Forensic Science", 9 *SCC J-18* (2023).
[113] Kuruma Kaniu v. The Queen, (1955) AC 197.
[114] Amazon Seller Services Pvt. Ltd. v. Directorate of Enforcement, writ petition (civil) no. 1082/2022.
[115] BSA, s. 57.

tampering.[116] If the chain of custody is broken at any stage, the admissibility of the evidence is thrown into question. Electronic evidence being a special case prominently need to be supplemented by proper chain of custody, and mere relevancy cannot suffice.[117] Chain of custody can be fairly maintained by keeping a record of who, what, when, and where handles the digital record and noting down each step of analysis along with its handling, transfer and storage.[118] Stricter rules for admissibility, along with clarity in requirements of procedure for producing electronic evidence as primary evidence should be laid down either through legislative enactment or through judicial pronouncement, as the Judiciary has recognized the need, for preservation, retrieval and production of digital evidence.[119]

Further, the admission of such records, unless proved to be primary and produced directly from the original device, needs to be mandatorily in accordance with **section 63(4) of the BSA, 2023.**[120] Though the courts have been highly receptive toward admitting electronic records as "document",[121] mere oral or secondary evidence for proving their authenticity may not be enough.[122]

The collection of digital evidence must also comply with the right to privacy and data protection,[123] fine-tuned with the spirit of Article 21. Proper guidance and training of investigators in-charge of conducting such investigations that involve data collection and storage may be necessary to not jeopardize data privacy.[124] A technical change in the functioning could include creating copies of the original work as soon as it comes under the control of the investigating agency and allowing the officers to only work with such "spare copies", preserving the original copy for production before the court.[125]

The need for improvement in infrastructural and institutional arrangement is also rampant to execute the vast scale changes in data collection, storage, transmission and disposal.[126] The authorities, officials, investigating officers, individuals seeking to produce digital evidence, need to be sensitized about the requirement of producing such evidence before the Court.[127]

Conclusion

The new criminal laws are India's attempt to de-stitch the colonial fabric from Indian laws and fill the gaps with contemporary provisions of law. Resultantly, the laws seem at par with global laws in the technological age with provisions for audio-video and electronic means for investigation, usage of digital forensics, and digital mediums of producing evidence before the court of law. However, whether these laws are fulfilling the standards of scrutiny set by the

[116] Nivrutti v. State of Maharashtra Through Police Officer and Anr., 2024 SCC Online Bom 3068.
[117] Archana Sarma, "Cyber Stalking and The Plight of Women in India- A Legal Perspective" 9 *RMLNLUJ* 175 (2017).
[118] Supra *Note* 94.
[119] Supra Note 10.
[120] Dhurben Guraldas Balani v. State of Gujarat, (2022) 1 GLH 680.
[121] Shamsher Singh Verma v. State of Haryana, (2016) 15 SCC 485.
[122] Supra Note 63.
[123] Science Direct *available at:* https://www.sciencedirect.com/science/article/abs/pii/S096969892300125X (October 14, 2024).
[124] Supra Note 107.
[125] Supra Note 76.
[126] Dr. G.K Goswami and Aditi Goswami, "Navigating Forensic Evidence under India's New Legal Landscape" 1 *SCC J* 7 (2024).
[127] Supra Note 89.

constitution to safeguard constitutional rights while ensuring administration of justice and procedural fairness is a matter to be considered in depth.

The BSA, 2023 embodies provisions for electronic records, audio-video recordings, any other computer outputs, to be produced as evidence. The most debated provision for admissibility of digital records is section 63(4) of the Adhiniyam, as per which, a certificate signed by an expert must be given along with the electronic evidence. The courts have pondered over the necessity of such a certificate and whether the need for it can be substituted by oral or any other kind of evidence. The most recent stance of the Apex Court culminated against such a stance, which establishes the necessity of the certificate as crucial.

Interestingly, India also introduced the DPDPA, 2023 which is a law, first of its kind, in regulating data privacy for India. It seeks to achieve in whole what the IT Act aimed to achieve with its amended provisions, to allow the processing of data as per constitutional norms and lay down guidelines for storing, transmitting, disposing, producing personal information. The cornerstone of the Act is founded on principles of data protection, with consent forming its bedrock. It is obvious that both legislations will have points of clashes in terms of one harping the production of digital evidence, even personal information and the other attempting to regulate data privacy.

The operation of a distinct mechanism for collection and processing of digital evidence would have to pass the constitutional test of validity to ensure that it is not breaching data privacy. The collection of evidence would have to be done according to a standard procedure to make sure the chain of custody is properly maintained, breach of data is prevented, and any alteration, modification or tampering is avoided. Further, the preservation of such data by organizations, authorities, or private individuals may constitutionally hamper the right of citizens to erase their personal information at their will. These worries need to be kept in mind while enforcing laws that carry a risk of breaching fundamental rights, even if the right itself may not be absolute.

Suggestions from the public and stakeholders can be taken for fruitful implementation and harmonization of the two laws. Adapting a standard operating procedure for investigation that results in collection of digital evidence, formulating transparent guidelines for, clear categorization between primary and secondary evidence, onboarding expert personnels for dealing with evidence that require extra caution, making institutional and infrastructural improvements, are some ways to accommodate the changes introduced under the new law. Awareness amongst investigative agencies and police personnel, on the need to respect data privacy and expand law enforcement mechanisms is the need of the hour.