International Journal of Humanities and Social Science Invention (IJHSSI)
ISSN (Online): 2319 – 7722, ISSN (Print): 2319 – 7714
www.ijhssi.org ||Volume 14 Issue 12 || December 2025 || PP. 49-55

Cybercrime Prosecution Gaps under IT Act and New Codes in India

Dr. Amit Kumar Bagaria
Assistant Professor (Law)
Govt. Law College, Sikar (Rajasthan)

Abstract
The present-day scenario of cybercrime prosecution in India forms the core of this research paper, which seeks to when discussed the IT Act 2000 and the new criminal codes of Bharatiya Nyaya Sanhita (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS), and Bharatiya Sakshya Adhiniyam (BSA) examine the "prosecution gaps" that have been generated. The controversy about overlapping jurisdictions and "double jeopardy" are consequences of the new laws that facilitate the country's legal system updating and at the same time allow the usage of digital evidence through procedural videography.
The investigation not only tackles the post-Puttaswamy dilemma and the Section 63 (BSA) evidence hurdle via hash value integrity but also draws the picture of the actual infrastructure shortages at the forensic science labs. By identifying the "practicality gap", which occurs when legislative demands surpass enforcement capacities, the research recommends a single "Cyber Procedural Code" and swift decentralization of forensics. In order to realize digital justice, it is crucial to find a middle ground between the rigorousness of procedures and the facilitation of technology.
Keywords: *Cyber-Legislative Overlap, Digital Forensic Integrity, Lex Specialis vs. Lex Generalis, Practicality Gap, Bharatiya SakshyaAdhiniyam (BSA)*

I. Introduction & Thesis Statement

The past few decades have seen an extraordinary transformation in the digital environment of India starting from almost none existent internet users in the late 1990's to one of the most populous online markets in the world. The rapid process of digital technology gaining acceptance has given rise to a difficult and even more series of cybercrimes taking-advantage-of the economy. The first legislative step was the IT (Information Technology) Act, 2000, which followed the UNCITRAL Model Law on Electronic Commerce[1]. The Act was first meant to aid in e-governance and the authentication of digital signatures but it was revised in 2008 to deal with more serious issues like cyber terrorism and identity theft[2].

The year 2024 at its very beginning heralded a significant change in the legal framework. The coming of the Bharatiya Nyaya Sanhita (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS), and Bharatiya SakshyaAdhiniyam (BSA) signaled a change in attitude as to the updating of Indian law along with the digital world. These reforms did not consist only of the mere adoption of digital realities; they went as far as a dramatic change throughout the whole legal system. Still, there is a big gap in "prosecution". This gap is not only caused by the old technology but is also rooted in the very conflict that lies between the provisions of the IT Act and the contemporary criminal codes.

Statement of Thesis

The criminal codes that have been introduced recently (BNS, BNSS, BSA) are aimed at modernizing the whole process of investigation and prosecution of digital crimes. On the other hand, the overlapping juristic area between the IT Act and the BNS and the strict procedural requirements of the BNSS have led to what is being called a "legislative paradox." Such a paradox is seen in lengthy procedures, conflicting accusations, and the existence of a gap where the digital demands of the law are beyond the capability of Indian law enforcement, which in turn, makes cybercrime prosecution more difficult.

Constitutional Framework

In India, the prosecution of cybercrimes has been influenced a lot by the debate between Article 21 (Right to Life and Personal Liberty) and the government's security concerns. The famous case of Justice K.S. Puttaswamy v. Union of India (2017) gave a strong vote for the Right to Privacy as one of the basic rights. The

[1]The Information Technology Act, 2000 (Act 21 of 2000).
[2]The Information Technology (Amendment) Act, 2008 (Act 10 of 2009).

Court also set out that any state interference in privacy must fulfill the three-part condition: Legality (there should be a legal framework), Legitimate State Purpose, and Proportionality (the ends and the means should be reasonably connected).

The Surveillance Paradox inside Novel Regulations

The enforcement of the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, has significantly increased the range of state surveillance[3]. On the one hand, the IT Act's Section 69 already allowed for interception and decryption of information, but the BNSS now provides a wider range of the procedural authorities involved in the matter. Whenever there are search and seizure activities, the provisions of Section 105 of the BNSS mandate that videography shall be conducted. While the whole idea is to ensure transparency, it automatically results in the collection of vast amounts of digital data that include people's biometric and personal living areas, and very often, no comprehensive data protection framework exists to stop potential misuse.

Besides, BNSS Section 173, the one that supersedes CrPC Section 154, allows the filing of electronic FIRs. The modernization here necessitates the obtaining of digital identities at the very start of a legal case. A constitutional problem arises when the so-called "predictive policing" and "real-time monitoring" aspects of BNS Section 46&111 in this way, which are here mostly labeled as measures against organized cybercrime, are introduced. These measures often bypass the privacy standard of "reasonable expectation" laid down in Puttaswamy[4].

Mandatory Disclosure and Self-Incrimination

The "compelled disclosure" of passwords and biometric security measures presents a major constitutional flaw. Per Section 94 of the BNSS, mirroring Section 91 of the CrPC, the court or police may call upon "any document or thing", which is now interpreted to cover digital devices. The Supreme Court ruling in Selvi v. State of Karnataka held that forced non-volitional testimony is a violation of Article 20(3) and 43 (Right against Self-Incrimination)[5][6].

The practical gap is clear: if a suspect was compelled to provide either his fingerprint or passcode for the purpose of unlocking a device containing incriminating evidence, would this act be considered "testimonial compulsion"? The new law has not really made it clear on this point and thus creating a gap where law enforcement usually resorts to coercive tactics which might in the end violate the "Just, Fair, and Reasonable" procedural standard that is required by Article 21[7].

In short, the new rules pass the "Legality" aspect of the Puttaswamy test, however, they still frequently fail the "Proportionality" test[8]. The absence of direct judicial oversight over digital search warrants, which is the situation in the United States and other countries, is a major constitutional weakness in India's battle against cybercrime[9].

Substantive Gaps: IT Act vs. BNS

The introduction of the Bharatiya Nyaya Sanhita (BNS), 2023, over the Indian Penal Code has not simplified the scenario rather it has created a tricky legal duality in respect of cybercrime punishment. The Information Technology Act, 2000, is considered the main "Special Law" (Lex Specialis) for computer-related crimes and is nevertheless the law of the BNS that has included within its "General Law" a number of digitally-native crimes. This intersection results in a considerable lack of individuals' rights especially concerning punishment, bail, and the legal principle of Generaliaspecialibus non derogant (special laws take precedence over general laws).

The Dilemma of Selection: Specific Legislation vs General Legislation

When an offense is classified under both Section 66D of the IT Act ("Cheating by personation using computer resource") and Section 319 of the BNS ("Cheating by personation"), a remarkable difference in legal interpretation arises. In the case of Sharat Babu Digumarti v. Government of NCT of Delhi (2016), the Supreme

[3]The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023).
[4]The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023).
[5]The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).
[6]Selvi v. State of Karnataka, AIR 2010 SC 1974.
[7]The Constitution of India, art. 21.
[8]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[9]Upendra Baxi, "On how not to judge the judges: Notes towards evaluation of the Judicial Role" 25 JILI 211 (1983).

Court ruled that the IT Act applies exclusively to electronic records and in that respect, it prevails over the general penal code[10].

The BNS further complicates the situation by specifically including "electronic means" in its definitions of organized crime (Section 111) and traitorous activities (Section 152). Prosecutors often prefer the BNS to the IT Act in order to avoid the bailable nature of charges under the IT Act. Most offenses under the IT Act are punishable with a maximum sentence of three years and are therefore bailable. In contrast, the BNS provisions for fraud or organized crime may impose much harsher, non-bailable sanctions. The law enforcement practice of "forum shopping" results in a scenario where justice is not uniformly administered, and thus, identical digital actions may lead to very different legal outcomes depending on the statute applied.

Redundant Definitions

The BNS introduces "Organized Crime" (Section 111), and within this, one of the principal parts is "cyber-crime." Nevertheless, besides the acts included under the IT Act, it does not give any further explanation about what "cyber-crime" really means. In this way, a large-scale phishing scam could be viewed as either a violation under Section 66D of the IT Act or as "Organized Cyber Crime" under BNS Section 111, resulting in confusion. The latter requires "syndicate" to be involved, but the definition of a syndicate in the digital space—where three people can share information on a dark-web forum—remains legally ambiguous.

The Discrepancy in Sentencing and Its Impact on Deterrence

The IT Act attracted criticism for being "too soft," since most of the offenses like hacking and identity fraud are bailable and usually lead to compounding (settlement). The BNS sets out to solve this problem through stricter punishments for traditional crimes, particularly those committed using digital channels.

Stalking: As per BNS Section 78 (formerly IPC 354D), cyber-stalking has been very specifically highlighted, with a penalty of up to 5 years imprisonment.

Data Theft: The BNS indeed confronts the problem of "damage to computer systems" in a rather interesting fashion by referring it to its Section 43/66 of the IT Act counterpart. In this way, data gets to be treated as "property," which opens up the possibility of applying the criminal breach of trust (Section 316) or theft (Section 303) that, while certainly less ambiguous and impractical in terms of proof and social stigma, have more legal and procedural implications.

Material Discrepancies

The main shortcoming is that there is no "Harmonious Construction" between the two laws. If the IT Act and the BNS are in conflict, the courts will be faced with a "Double Jeopardy" situation. For example, in case a person is acquitted under the IT Act because of a flaw in the digital forensics, will he/she still be subjected to prosecution for thehidden corrupt acts under the BNS? Modern legal principles suggest no; however, the broad language of the BNS attracts these situations and thus there will be prolonged litigation and no clarity of law for both the criminal and the victim[11].

Procedural Gaps: BNSS & Investigation

The Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, introduces a technology-driven approach for the criminal process; however, it creates a lot of operational ""frictions"" when dealing with the invisible side of cybercrime. The migration from the CrPC to the BNSS was supposed to speed up the investigation; nevertheless, the new procedural requirements often clash with the technical difficulties of digital forensics and the basic anonymity of the internet.

The Compulsory Videography Requirement (Section 105)

The most notable alteration brought about by the BNSS is Section 105 which stipulates that the entire search and seizure process along with the seizure list's production should all be "audio-video electronically" documented, preferably to a mobile phone.

The Practical Gap: In the case of conventional physical searches (for instance, getting a weapon), it is very easy to film the process. When it comes to cyberspace crimes, the term "seizure" often means "making an exact copy" of a hard drive or collecting volatile data from RAM. Recording the activity of a forensic expert giving commands on a computer for six hours is not only extremely tiring but also creates a risk of exposing the secretive methods of the investigation along with the passwords that might have been captured on video. Additionally, if due to a technical defect or battery flatness, an officer does not capture the seizure, the

[10]Sharat Babu Digumarti v. Government of NCT of Delhi, (2017) 1 SCC 18.

[11]The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

Allahabad High Court in Shadab v. State of U.P. (2025) has indicated that such non-compliance could be a ground for bail thus allowing sophisticated cybercriminals to take advantage of the loopholes in the process.

Digital "Property" and the Scope of Section 107

The BNSS expands considerably the definition of property to obviously include digital and electronic assets. The protocol for confiscation of such property is set out in Section 107. However, it does not imply Data Integrity technical standards. Digital Evidence is "fragile" as opposed to physical evidence; even the very first boot-up of a seized computer could alter metadata (including last accessed dates), thus putting the evidence's admissibility at risk. The absence of a "Digital Chain of Custody" procedure is one of BNSS's drawbacks, thus law enforcement has to rely on old standing orders that have not been changed in accordance with the recent Sanhita regulations.

The Dilemma of Anonymity and Electronic FIRs (Section 173)

The BNSS sets the e-FIR in stone (Section 173), which in turn allows the victims to report the crimes committed against them electronically. This, on one hand, provides better accessibility to offenders but on the other hand, this leads to a "Verification Gap." Cybercriminals are usually inclined towards exploiting the use of a VPN, utilizing TOR browsers, and creating fake identities. The BNSS law asks the informer to allow the e-FIR within a period of three days. The requirement of a three-day physical signature creates a bottleneck in the procedure when the victim is in a different state or in the case where the crime involves an anonymous whistleblower, which sometimes leads to the FIR being dismissed and the perpetrator getting enough time to erase digital evidence[12].

Coerced Decryption and Privacy

There is a big disparity of opinion on the topic of Anonymity and Encryption. The Basic National Security System (BNSS) has the power to "produce electronic devices" (in Section 94), but it is still not clear whether or not a suspect could be forced by law to give a decryption key or biometric unlock[13]. The transition of cybercrime to totally encrypted channels (e.g. Telegram, Signal) has resulted in a stalemate because there are no clear procedural regulations regarding "Compelled Decryption." Law enforcement officials very often have the devices they cannot open, but the courts are very careful not to break the "Right to be Forgotten" or the right against self-incrimination[14].

Infrastructure and Forensic Capability

Talking about the cybercrime area, every "crime scene" is absolutely digital. Currently, India is facing a huge shortage of certified cyber-forensic examiners. The presence of a forensic expert in every major data leak or financial fraud trial is nothing more than a "luxury" that the already burdened legal system, with so many cases piled up at State Forensic Science Laboratories (FSLs), cannot afford. This situation gives rise to what can be termed as "Delay Gap," in which digital evidence is kept for months or even years without examination, thus, losing its importance in the rapidly developing tech world.

The Evidentiary Hurdle: BSA & Sec 65B/63 (Admissibility issues)

The BSA, 2023, replaces the Indian Evidence Act, 1872, with the intention to give electronic data the same legal recognition as paper documents. The shift from the notorious Section 65B of the old law to Section 63 of the BSA has opened up new evidence-related issues that could dramatically impact the number of cybercrime convictions in the future[15].

Transition from Secondary to Primary Evidence

The electronic records were usually treated as secondary evidence under the old regime. Therefore, for the records to be admissible under Section 65B (4), a certificate was a must. The BSA brings in a new system: still, Section 57 (Explanations 4 to 7) considers some electronic and digital data as primary evidence. This means that if the "original" digital record is produced by the particular device used for creating the data, there will be no need for a certificate[16].

[12]Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
[13]Ministry of Home Affairs, "Standing Committee Report on the Bharatiya Nagarik Suraksha Sanhita" (August, 2023).
[14]Shreya Singhal v. Union of India, AIR 2015 SC 1523.
[15]Law Commission of India, "271st Report on DNA Profiling" (July, 2017).
[16]Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801.

The Practical Gap: In a cybercrime case, the original is not a single physical item; rather, it is commonly spread out over different locations like cloud servers or temporary memory. If a lawyer claims that a WhatsApp conversation is "Primary Evidence" just because he has the phone, while the opposing lawyer argues that the conversation was "copied" from the server to the phone, it will be up to the court to decide if the Section 63 certificate is still required. This uncertainty might bring back the whole "technicality vs. justice" debate which the Supreme Court tried to settle in Arjun Panditrao v. Kailash Kushanrao (2020)[17].

The Revised Dual-Certificate Mandate

The new Schedule associated with the Act now requires a bifurcated certificate instead of one whole. Section 63(4) of the BSA creates a more stringent certification procedure.

1. Section A: To be filled in by the person who is in charge of the device.
2. Section B: To be filled in by a Specialist.

The Prosecution Gap: The BSA does not clarify at all what the criteria are for being a "specialist" in Part B. India currently lacks the trained men who could validate the certificates for the huge number of electronic records produced in courts daily, considering the "Examiner of Electronic Evidence" as mentioned in Sec 79A of the IT Act. The "Expert Bottleneck" can lead to a situation where digital evidence like emails, logs, and CCTV footage is not taken into account simply because there was no certified expert available to sign the form when the charge sheet was filed[18].

Hash Value Protocols

In an unprecedented manner, the mandated format for the certificate (as prescribed by the BSA Schedule) now requires the presentation of Hash Values (digital fingerprints). This is a good step forward for data integrity, but it also creates a "Practicality Gap" for local police. A vast majority of law enforcement officials are not equipped with the skills to create MD5 or SHA-256 hashes during the time of seizing the evidence. If the original certificate does not have the hash value or has an incorrectly calculated one, the whole digital record may be considered "tampered with" and excluded from evidence, regardless of the proof's validity[19].

To sum up, the BSA keeps on changing the vocabulary of the evidence while at the same time raising the bar for "procedural perfection." In a country where a common investigative officer has no access to high-tech forensic skills, such new challenges to evidence may mistakenly provide a "procedural escape hatch" for computer hackers who are skilled.

Practicality & Ground Reality (Infrastructure & Forensic Gaps)

The Bharatiya Nagarik Suraksha Sanhita (BNSS) and Bharatiya SakshyaAdhiniyam (BSA) do create an advanced legal framework, however, the discrepancy between the infrastructure and the processes is the main factor that holds back the conditions of cybercrime prosecution in India. The success of any cyber prosecution relies on the speed of digital evidence extraction and the investigator's technical skill—two areas where India is currently facing a major downfall[20].

The Forensic Backlog and the Scarcity of "Experts"

The services offered by forensic science laboratories (FSLs) differ significantly from the mandatory ones for crimes under Section 176 of the BNSS with penalties of seven years or more. On the contrary, the processing times of these cases have grown due to the radical increase of over 900% of the case load in 2021, which has also made it impossible for the government to expand the National Cyber Forensic Laboratory (NCFL) network before the completion of the new facilities in Delhi and Assam by 2025. In several state-run forensic science laboratories, the time required to obtain a forensic report of a confiscated mobile device could be as long as 18 to 24 months. In the digital world, where new software and encryption technologies come out every month, a two-year-old forensic report is often regarded as technically outdated by the time it gets to court.

The Discrepancy Between Training and Technology at Police Stations

The number of people trained through the CCPWC initiative and the CyTrain MOOC platform is over 24,600, yet this figure is only a tiny fraction of the total number of police officers in India, which is 1.5 million. The local Thana level is where the "Practicality Gap" is felt most strongly. The majority of the investigative officers are lacking the advanced forensic workstations, licensed extraction tools like Cellebrite, and reliable

[17]Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
[18]State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.
[19]Bureau of Police Research and Development, "Handbook on the Bharatiya Nyaya Sanhita, 2023" (2024).
[20]Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

internet connections that are necessary for uploading the evidence to the Samanvaya MIS platform. This situation forces local police to resort to private forensic consultants, the results of whose work are sometimes disputed by the defense lawyers because of lack of official "accreditation" under Section 79A of the IT Act.

Issues in Data Instability and Storage

The BNSS mandate for video graphing searches (Section 105) creates a secondary infrastructure crisis: Digital Storage. Police departments require a large and secure cloud infrastructure to store the large number of high-definition video evidences taken during each raid. When there is no centralized and encrypted "Evidence Management System," this material is often kept on local drives without protection, which puts its integrity at risk and makes it subject to permanent loss, thus the prosecution's case might fail because of the strict admissibility standards of the BSA.

Cross-Border Viability

The global nature of cybercrime is the main practical difficulty that is most important. The Samanvaya platform allows for interstate connections but still, most cyber-frauds come from "hotspots" that mislead the law. The I4C has been signing MoUs with international institutions like the US Department of Homeland Security in 2025, but still, the process of getting information from foreign intermediaries like Google, Meta, or Telegram remains a bureaucratic nightmare. Mutual Legal Assistance Treaties (MLATs) may take months or even years to complete, during which the evildoer often wipes out the "digital trail."

II. Conclusion & Recommendations

An extraordinary effort will be made in digitizing Indian criminal law through the transition to the Bharatiya Nyaya Sanhita (BNS), BNSS, and BSA in the years 2024-2025. Accordingly, the application of our study illustrates the grand disparity in the will of the legislator and the actual execution. The court's evidence standards set by BSA, the sharing of jurisdictions between the IT Act and the BNS, and other reasons have led the legal process to favor technicalities instead of substantially just outcomes.

The aftermath of these possible gaps in the prosecution invites the following changes accordingly:

1. In order to clear out the "Special vs. General Law" issue in India, the whole country's procedures for overall handling on cyber cases should be united and solely made to work with the IT Act.
2. The government should not waste time in releasing the ₹30,000 crore budget for setting up forensic universities and mobile units in each district, as per the Standing Committee on Home Affairs' recommendation made in August-2025, in order to take care of the most soon 18–24-month evidence backlog.
3. The 2026 Supreme Court ruling signifies that it is very vital to the establishment of a standard operating procedure (SOP) for the digital evidence handling to ensure the procedural justice, particularly with regard to the account freezing and "Hash Value" protocols.
4. The staggering 250% increase in financial frauds calls for the setup of cyber-courts with judges having technical specialization and "Expert Witnesses" (as outlined in BSA Section 63) by their side.

The new regulations establish the "skeleton" of a contemporary system, but to assure a safe and creative digital future for India, it is imperative to reinforce the "muscles"—infrastructure, capacity building, and international cooperation.

Reference

[1]. The Information Technology Act, 2000 (Act 21 of 2000).
[2]. The Information Technology (Amendment) Act, 2008 (Act 10 of 2009).
[3]. The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023).
[4]. The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023).
[5]. The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).
[6]. Selvi v. State of Karnataka, AIR 2010 SC 1974.
[7]. The Constitution of India, art. 21.
[8]. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[9]. Upendra Baxi, "On how not to judge the judges: Notes towards evaluation of the Judicial Role" 25 JILI 211 (1983).
[10]. Sharat Babu Digumarti v. Government of NCT of Delhi, (2017) 1 SCC 18.
[11]. The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
[12]. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
[13]. Ministry of Home Affairs, "Standing Committee Report on the Bharatiya Nagarik Suraksha Sanhita" (August, 2023).
[14]. Shreya Singhal v. Union of India, AIR 2015 SC 1523.
[15]. Law Commission of India, "271st Report on DNA Profiling" (July, 2017).
[16]. Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801.
[17]. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
[18]. State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.
[19]. Bureau of Police Research and Development, "Handbook on the Bharatiya Nyaya Sanhita, 2023" (2024).
[20]. Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

Bibliography

A. PRIMARY SOURCES: STATUTES & CONSTITUTION

1. The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023). [Available at: https://www.indiacode.nic.in/handle/123456789/20099]
2. The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023). [Available at: https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf]
3. The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023). [Available at: https://www.indiacode.nic.in/handle/123456789/20063]
4. The Constitution of India, 1950. [Available at: https://legislative.gov.in/constitution-of-india/]
5. The Digital Personal Data Protection Act, 2023 (Act 22 of 2023). [Available at: https://www.indiacode.nic.in/handle/123456789/22037]
6. The Information Technology (Amendment) Act, 2008 (Act 10 of 2009). [Available at: https://www.meity.gov.in/writereaddata/files/it_edit.pdf]
7. The Information Technology Act, 2000 (Act 21 of 2000). [Available at: https://www.indiacode.nic.in/handle/123456789/1999]

B. JUDICIAL PRECEDENTS

1. *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.
2. *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
3. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
4. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
5. *Selvi v. State of Karnataka*, AIR 2010 SC 1974.
6. *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801.
7. *Sharat Babu Digumarti v. Government of NCT of Delhi*, (2017) 1 SCC 18.
8. *Shreya Singhal v. Union of India*, AIR 2015 SC 1523.
9. *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600.

C. REPORTS & SECONDARY SOURCES

1. Baxi, Upendra, "On how not to judge the judges: Notes towards evaluation of the Judicial Role" 25 *Journal of the Indian Law Institute* 211 (1983).
2. Bureau of Police Research and Development, "Handbook on the Bharatiya Nyaya Sanhita, 2023" (BPR&D, New Delhi, 2024). [Available at: https://bprd.nic.in/uploads/pdf/BNS%20Book_After%20Correction.pdf]
3. Law Commission of India, "271st Report on DNA Profiling" (July, 2017). [Available at: https://lawcommissionofindia.nic.in/reports/Report271.pdf]
4. Ministry of Home Affairs, "Standing Committee Report on the Bharatiya Nagarik Suraksha Sanhita" (August, 2023). [Available at: https://prsindia.org/files/bills_acts/bills_parliament/2023/Joint_Committee_Report_BNSS.pdf]