Page 3243 - 3251 **DOI:** *https://doij.org/10.10000/IJLMH.119419*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 2

2025

Unravelling the Misinterpretations Surrounding Search and Seizure Provisions: The Endangered Side of Criminal Procedure

ARSHYA WADHWA[1]

ABSTRACT

This paper critically examines the evolving challenges of search and seizure procedures in the context of criminal law and the current digital age, with a special focus on the shift from the Code of Criminal Procedure, 1973 (CrPC) to the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS). It explores the extent to which these legal frameworks address or rather fail to address the complexities of the digital era, where technology has significantly reshaped both privacy and investigative processes. Through a constitutional lens, particularly Article 21 and the jurisprudence on the right to privacy, the paper questions whether procedural safeguards have meaningfully evolved to keep pace with the intrusive capacities of digital surveillance and forensic technologies.

By analyzing key cases such as the infamous Bhima Koregaon arrests, the paper reveals the systematic risks of misusing search and seizure powers, especially in cases involving digital evidence. It argues that the lack of statutory clarity on digital searches leaves individuals vulnerable to overreach and violation of due process. The BNSS, despite its promise of an 'anti-colonialist' structure, continues to carry forward ambiguities and archaic assumptions from the CrPC, missing an opportunity to strengthen rights-based protections in the investigative process.

The paper also examines the role of investigative often with little judicial oversight. This raises serious concerns regarding evidentiary authenticity, potential planting or manipulation of data, and overall accountability. Ultimately, the paper urges for a reimagination of procedural law that aligns with the digital realities of the current era. It advocates for interpretive sensitivity from courts, legislative specificity on digital search protocols, and stronger data protection norms to uphold the rule of law and prevent the erosion of civil liberties under the guise of national security or public order.

Keywords*: Search and Seizure, Data Privacy, Criminal Procedure, Constitutional Rights, Right to Privacy, State Surveillance.*

[1] Author is a student at O.P. Jindal Global University, India.

 [ISSN 2581-5369]

I. INTRODUCTION

The eruption of digital revolution in our lives has prompted a series of legal debates especially in the realm of criminal laws. The Code of Criminal Procedure (hereinafter, "CrPC") which is a British made law that could not foresee and keep up with technological advancements. Under the CrPC, chapter VII deals *with processes to compel production of things* which remains unclear till date regarding the inclusion of electronic evidence and how it must be dealt with. Unfortunately, due to a multiplicity of cases involving a political angle by nature, certain procedural provisions from the CrPC have appeared to be misused by the hands of the police officers. For instance, in the infamous Bhima Koregaon case[2], there was a massive ignorance of the criminal procedure laws by the police regarding the search and seizure of electronic evidence. This is one case because of which certain targeted individuals' digital devices were taken in custody leading to a subsequent violation of their fundamental right to privacy. The Bhima Koregaon case is an unfortunate reminder to the procedural inconsistencies present in our system especially when those speaking up against the government are the constant and most accessible targets to an already existing weak system. The lack of clarity in the CrPC regarding search and seizure of digital devices has the potential of further leading to miscarriage of justices especially against those certain dissenting individuals. Flowing from the background of these events, this paper will be delving into firstly, the adequacy of current laws to compel digital content, secondly, the misapplications of the search and seizure procedure in the Bhima Koregaon case furthering the ill-treatment of the vulnerable, thirdly, the departure from CrPC to BNSS in terms of search and seizure provisional changes along with the proposed guidelines to reform the system overall and lastly, a conclusive remark with a tentative suggestive framework.

Research question: How have the interpretations of search and seizure provisions of the CrPC compromised the privacy, security and data protection of individuals? Explain why this poses a matter of legal concern as this has put certain targeted individuals'\groups' privacy in danger. Elaborate on the recent legislative and judicial enhancements which could effectively address the search and seizure procedures.

(A) Are the current provisions adequate for compelling production of digital devices?

Currently, two major provisions, namely Section 91 and Section 93 of the CrPC deal with the

[2] Goyal, P. (2021). *Bhima Koregaon case: Three years of legal and rights violations*. Newslaundry. https://www.newslaundry.com/2021/01/02/bhima-koregaon-case-three-years-of-legal-and-rights-violations

 [ISSN 2581-5369]

aspect of search and seizure under compelling things or documents. Section 91[3] mentions "summons to produce document or thing" which has been deemed to be broad in its application. Wherein in Section 93, the circumstances under which a search warrant may be issues is mentioned.[4] There have been contentious issues laid down with Section 91 and its application especially in the area of digital devices in the ambit of the provision. The courts' stance on the interpretation of section 91 and whether it should include electronic material has varied across jurisdictions and rendered to be contradictory. Scholars have noted that Indian courts have taken liberty in including electronic contents such as CDs etc. under the purview of 'documents'. Whereas certain courts have limited the understanding of section 91 to physical things only. Nonetheless, the revamping of the old criminal laws with the new ones have brought changes within their digitised versions. The Bhartiya Nagarik Suraksha Sanhita (BNSS) as a replacement to the CrPC has interchanged Section 91 with Section 94 wherein additions of electronic communication have been made. Keeping this in our conscience, the aspects of BNSS will be elaborated further after having discussed the provisions of CrPC based on which certain interpretations (and misinterpretations) in the existing system have taken place.

Scholars such as Tarun Krishnakumar have also argued that the ambit of Section 91 in terms of production of data has been widely interpreted by the courts. When it comes to production of those things which are digital in nature and possess data, third parties such as intermediaries can also produce them apart from the parties involved. Although the Supreme Court have provided such third parties with a remedy wherein, they can file revision petitions against such orders. The implications of such orders are dire when it comes to privacy and data protection. Additionally, the issue arising from noncompliance with Section 91 order due to inconvenience was declared as an invalid excuse by the Allahabad High Court in the case of Surendra Mohan v. K.P.M Tripathi. This principle may not make it easy for the recipients of Section 91 to argue their case in terms of compliance with order being burdensome. Thus, the principle is extremely open ended for the courts to interpret it according to the facts and circumstances of particular cases. [5]

Some of the impertinent concerns regarding Section 91 have been mentioned above as laid down by scholarly interpretations. However, one major concern pertaining to Section 91 is the inconsideration toward a potentially accused person's privacy. Although the provision has

[3] S.91, Code of Criminal Procedure 1973
[4] S.93, Code of Criminal Procedure 1973
[5] Krishnakumar, T. (2022). *Law Enforcement Access to Data in India: Considering the Past, Present, and Future of Section 91 of the Code of Criminal Procedure, 1973*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4154589

 [ISSN 2581-5369]

explicitly mentioned "necessary and desirable" as preconditions before any production of document or thing, the application might differ for physical things as a contrast to digital things. Due to the lack of presence of any form of digital evidence being mentioned in Section 91, the provision has created a legal loophole by granting unfettered powers to the police to seize electronic items without any statutory safeguards against such acts. Subsequently, the aspect of privacy becomes pivotal when the search and seizure of electronic devices is considered. Electronic items such as mobile phones, laptops and so on contain personal information of individuals which may not be related to the respective case, yet their information could be at scrutiny by the officials handling it. Moreover, without properly distinguished laws on seizing digital devices as compared to physical things, it would be difficult to establish certain safeguards against the former. In India, we have seen certain cases wherein this legal complexity has led to the perusal of certain vulnerable sections of the society.

II. THE APPLICATION OF SEARCH AND SEIZURE: A SHAM IN THE NAME OF DUE PROCESS

The inadequacy of the search and seizure provision of CrPC has led to allegedly massive injustices in one of the most controversial cases which is popularly known as the Bhima Koregaon case.[6] Several activists were charged with offences laced in the Unlawful Activities (Prevention) Act, 1967[7] wherein major malpractices by the police and investigative agencies was alleged by the accused persons. One of the accusations against the police was that upon seizing the electronic record, the police did not gather digital signatures to prove its authenticity as prescribed under the Information Technology Act, 2000 (hereinafter IT Act)[8]. This led to a suspicion of evidence tampering at the hands of the police and the accused person's advocate also argued that sealing of electronic devices does not guarantee protection of data given the volatile nature of technology.[9] Additionally, there have been multiple alleged spyware attacks on the accused persons of the Bhima Koregaon case which have compromise the state of their digital devices and the data within it. [10] These are some of the areas wherein the law has faltered in mentioning the safeguards against the aspect of privacy of individuals whose electronic records are to be seized by the police officers. Another crucial procedural irregularity in the same case has been observed regarding the police raids into the houses of the persons who were

[6] Romila Thapar & Ors v. Union of India & Ors 2018 SCC OnLine SC 1961
[7] Unlawful Activities (Prevention) Act, 1967
[8] s.3A Information Technology Act, 2000
[9]Ganesan, A. (2023). *Bhima Koregaon seized devices not properly secured: Lawyer*. MEDIANAMA. https://www.medianama.com/2023/10/223-anand-grover-bhima-koregaon-seized-devices-security/
[10]Jain, M. (2021). *Jailed activist Rona Wilson's phone was compromised with Pegasus spyware: Report*. MEDIANAMA. https://www.medianama.com/2021/12/223-rona-wilson-phone-compromised-pegasus-report/

 [ISSN 2581-5369]

involved in this case. After having been twice denied a search warrant by the Judicial Magistrate First Class, the investigating officer raided the houses of a lawyer and two activists seizing their electronic devices which included computers, laptops, pen drives, portable device and so on. [11]This is an utter disregard and disrespect by the police toward the magistrate's order which explicitly denied the search warrant. Unfortunately, the unclear nature of the law in such cases wherein there is so punitive action toward police officials for disregarding the law blatantly makes the machinery an extremely strong one with most powers at their helm. The officer had made the request of the search warrant in front of the magistrate laying a claim that the accused persons will not coordinate which was considered baseless by the magistrate, hence leading to a refusal in giving search warrant.

Moreover, due to the technicalities involved in confiscating digital evidence, this case highlights the anomalies which were reported by certain journalists. After following the legal procedure in tandem with the IT Act, the electronic devices once seized must be sealed to ensure that there is no evidence tampering or interference by the police officers. However, in this case, the time stamps on the memory card's video recording showed its las access to be after the seizure and sealing had been done, as per the forensic reports. [12] It has also been noticed that the computer system of one of the accused persons was seen to be switched on post seizure procedure was complete without any justification or reasoning by the police officer. These are some serious contentions which go unnoticed in such cases where the sentimental value is higher than the technical errors against the accused persons. On top of that, there is a paucity in procedural safeguards against such seemingly minor errors which may play a huge role in the subsequent hearings of the case. What makes this case poignant is firstly the fact that most of the accused persons belonged to professional groups such as lawyers, activists, journalists and professors who belong to human rights groups and have outwardly spoken against the status quo of the government. Secondly, the interesting aspect is that the police had solely relied on electronic evidence which led to the arrest of the accused persons. The sole reliance on electronic evidence which has gone under scrutiny by organisations like amnesty international along with the disregard of law on multiple counts as envisioned by the facts makes the suspicions appear reasonable in doubting the misapplication of Section 91 as the search and seizure provision majorly highlighted throughout. Thirdly, the copies of the electronic records were given to the

[11]Goyal, P. (2021b). *Bhima Koregaon case: Three years of legal and rights violations*. Newslaundry. https://www.newslaundry.com/2021/01/02/bhima-koregaon-case-three-years-of-legal-and-rights-violations

[12] Shantha, S. (2019). *Bhima Koregaon: Amid Demands For Fresh Probe, A Hard Look at the Case's Discrepancies*. The Wire. https://thewire.in/rights/discrepancies-bhima-koregaon-investigation-sharad-pawar-demands-fresh-probe

accused parties much later as well, again raising doubts upon the authenticity and trustworthiness by the police. Fourthly, apart from the search and seizure misapplications, there was also a disregard toward Section 100(4) wherein the police must involve independent and respectable persons of the society before searching a locality (in this case, the raids which took pace). However, it was found out that the Pune police had their own 'stock' witnesses which compromised the rationale behind Section 100(4).[13]

The incongruencies in the Bhima Koregaon case signify the need for having an overall better procedural system to produce digital evidence. Human rights violations do not occur in a vacuum and fair procedures play an important role in deciphering the fate of the parties involved in cases involved nationalist sentiment and individual freedom. The accused persons in the case had to suffer massively due to a compromise on their fundamental rights, especially right to privacy under Article 21[14] and right against self-incrimination under Article 20(3)[15] which is intertwined with one another. However, in December 2023, the BNSS was passed by both the houses of the parliament as a replacement to the archaic British made CrPC. This led to inclusion of digital facets being acknowledged in the new criminal act wherein a major shift was noticed under the search and seizure mechanism, earlier missing in the CrPC. However, whether the updated version with addition propose any different to the existing concerns regarding privacy and data protection is an important question to pose given the digital paradigm shift.

III. THE INTERPLAY OF CRPC REPLACEMENT (BNSS) AND DRAFT SEARCH AND SEIZURE GUIDELINES

The proposed changes in the BNSS from Section 91in the CrPC to Section 94 in the BNSS now includes digital evidence in its ambit explicitly which encompasses any *electronic communication including communication devices which is likely to contain digital evidence.* As progressive as the new addition might sound, the problem of the loopholes mentioned above in the case and especially those pertaining to privacy remain unanswered. The new provision simply means that now the court or police officer in charge can summon any electronic communication which could include audio or video recordings, messages, emails, call recordings etc., as well as devices which enable electronic communication such as laptops, mobile phones, cameras and so on. Certain concerns were pointed out by such a definition as well by Derek O'Brian which broadly pertained to the invasion of privacy given the massive

[13] s.100(4) Code of Criminal Procedure, 1973
[14] a.21 The Constitution of India, 1950
[15] a.20(3) The Constitution of India, 1950

 [ISSN 2581-5369]

amount of personal information present in digital devices. Additionally, an important criticism mentioned by him was regarding the access to such devices which could render compromising the right against self-incrimination specified in Article 20(3) of the Indian Constitution.[16] For the first concern regarding the privacy of individuals being compromised has the potentiality of jeopardising an individual's entire case. The possibility of this has been highlighted in the controversial case above and its futuristic possibility even with the advent of BNSS is inevitable. This is because the Section 94 of the BNSS does not mention *what kind of* evidence would render to be relevant to the particular case. If the ambit is as broad as how the new law mentions it to be, the ambiguity might make the enforcement agencies and officers to exercise unbalanced powers. Subsequently, if the relevancy of any and every communication between individuals is scrutinised, the insignificant bits could be taken out of context putting accused persons into a vulnerable position and more difficult to defend themselves. Moreover, the fundamental right to privacy of individuals as enshrined in the famous Puttaswamy judgement would be highly violated given the volatile nature of data present in communication devices.[17]

The second concern regarding self-incrimination pertaining to the procedure involving the access of digital devices is an extremely tricky one as well. The main issue in such cases arises regarding the testimonial nature of passwords and/or biometrics to unlock devices of individuals and whether that is incriminatory or not. In the case of Selvi v. State of Karnataka,[18] the Supreme Court acknowledged the treatment of passcode/biometric as testimonial evidence as opposed to what the High Court had laid down. The court laid out salient principles through this case wherein they recognised the aspect of "mental privacy". The Supreme Court considered the High Court reasoning flawed wherein the latter considered the password as a corollary to the word document in Section 91. The Supreme Court rectified this erred justification and elucidated that the unlike physical evidence, the password forms a part of someone's personal information which is to be protected under Article 20(3) of the Constitution. Similarly, the Supreme Court highlighted another error by the subordinate court pertaining to the misinterpretation of Section 93 of CrPC dealing with the issuance of search warrant. Herein, the word "place" in the provision could not replace a mobile phone or a laptop especially when

[16] M, S. (2023). *Device seizure rules in BNSS violate right to privacy: Derek O'Brien*. MEDIANAMA. https://www.medianama.com/2023/11/223-device-seizure-right-to-privacy-derek-obrien-dissent-note-2/

[17] Panigrahi, P., & Mehta, E. (2022). *THE IMPACT OF THE PUTTASWAMY JUDGEMENT ON LAW RELATING TO SEARCHES*. NUJS Law Review – The Quarterly Flagship Journal of NUJS. http://nujslawreview.org/wp-content/uploads/2022/07/15.1-Panigrahi-Mehta-3.pdf

[18] Selvi v. State of Karnataka 2013 SCC OnLine SC 1388

the definition of "place" has been mentioned in the CrPC. [19]

In the light of the dreary events pertaining to lack of privacy due to arbitrary application of search and seizure laws, the Supreme Court has entertained a couple of cases addressing this concern. The Court clubbed the petition filed by the Foundation for Media Professionals (FMP) with the pre-existing Ram Ramaswamy v. Union of India[20] case, wherein both had similar demands, seeking guidelines for search and seizure of electronic devices. [21] The advocate for the petitioned laid out some guidelines for the betterment of search and seizure procedures in order to avoid excess power in the hands of law enforcement agencies. Some of the important aspects of the guidelines include[22]: firstly, the judicial warrant must be a rule except in emergency situations; secondly, the warrant application must contain all the relevant information; thirdly, an independent agency should examine the device within 24 hours of seizure; fourthly, the owners must have a right over removal of any irrelevant information from the device under the supervision of independent agency; fifthly, owners cannot be forced to share the passcodes of their devices and lastly, data retention guidelines also find a mention in the suggested framework. [23]

IV. CONCLUSION

The rise of this digital age has also birthed unique forms of concerns which have the potential of threatening a person's existence all together. Data privacy plays an integral role in our lives given the rampant usage of electronic communication devices impertinent in our day-to-day businesses and leisure time. Moreover, certain outdated criminal procedural laws may not be in consonance with the forthcoming tensions anticipated by these technological reforms. Search and seizure of electronic devices and communications is one such inevitable grey area in the Indian legal landscape which now finds acknowledgement in the new BNSS, however, finds no adherence to the safeguarding principles against its implementations. The argument throughout the paper has not been regarding the mere acknowledgment of digital devices in the criminal procedure but making the law wholly encompassing of all the privacy concerns of individuals.

---

[19] Mody, A., & Sijoria, S. (2023). *Right of Self-Incrimination in Digital Age: Whether Compelled Disclosure of Password/Biometrics is Unconstitutional? | SCC Times*. SCC Times. https://www.scconline.com/blog/post/2023/03/18/right-of-self-incrimination-in-digital-age-whether-compelled-disclosure-of-password-biometrics-is-unconstitutional/

[20] Ram Ramaswamy v. Union of India 2023 SCC OnLine SC 1703

[21] *Guidelines for search and seizure of digital devices - Supreme Court Observer*. (n.d.). Supreme Court Observer. https://www.scobserver.in/cases/guidelines-for-search-and-seizure-of-digital-devices/

[22] '*Supreme Court Circulates Interim Guidelines for Seizure of Devices*. (2023). The Wire. https://thewire.in/rights/supreme-court-circulates-interim-guidelines-for-seizure-of-devices

[23] Sanzgiri, V. (2023). *Interim search and seizure guidelines submitted before SC*. MEDIANAMA. https://www.medianama.com/2023/11/223-interim-search-and-seizure-guidelines-sc-2/

 [ISSN 2581-5369]

As seen in the case mentioned above, the Bhima Koregaon irregularities are one of the many examples wherein procedural injustices can cause derails in the trial henceforth also threatening the already vulnerable sections of the society with excess state surveillance and unnecessary policing of one's digital possessions. In order to avoid such situations, the judiciary must incorporate the draft guidelines presented in the combined cases as mentioned above. Additionally, the legislature would also have to ensure that their newly drafted laws (particularly Section 94 of BNSS) leaves no room for misinterpretation of such wide clauses wherein an individual's data privacy is at stake. Thus, an aim for a balanced approach regarding integrity of criminal proceedings and protection of individuals shall be made by the judiciary whilst considering adopting the new search and seizure guidelines. Be that as it may, in the current digital age wherein our dependency on electronic media has augmented, our fundamental rights are more at risk than ever. Thus, in order to maintain the constitutional sanctity of such rights and law enforcement, due process should be adhered to especially by the state authorities. Most importantly, a particular statute does not get implemented in a vacuum, there is a combination of laws which come to place in its application. Some forms of excess state involvement have been observed in the Digital Personal Data Protection Act, 2023, which would make it more difficult for those fighting for their data privacy rights.[24] Nonetheless, the CrPC acting as a backbone of the criminal procedures in most cases, must be adhered to with specific guidelines and strict implementation policies for search and seizure of electronic mediums.

*****

[24] Kodali, S. (2023). *Ten Reasons Why The Digital Personal Data Protection Law Doesn't Empower Citizens*. The Wire. https://thewire.in/law/will-the-data-protection-law-empower-the-public

 [ISSN 2581-5369]