INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

DIGITAL POLICING AND THE RIGHT TO FAIR INVESTIGATION: AN ANALYSIS UNDER THE BHARATIYA NAGARIK SURAKSHA SANHITA, 2023

AUTHORED BY - SAMBHAV SINGH & DR. ARVIND KUMAR SINGH
Amity University Lucknow Campus

Abstract

The criminal justice system of any country depends heavily on the fairness of its investigation process. In India, the Constitution guarantees the right to life and personal liberty under Article 21.1. Over time, the Supreme Court has interpreted this right to include the right to a fair investigation. This means that the police must investigate crimes honestly, without bias, and by following proper legal procedures. If an investigation is unfair, the entire criminal process becomes unreliable, even if the trial appears to be fair.

In recent years, policing in India has undergone rapid changes due to the use of digital technology. Police investigations now rely on electronic records such as mobile phone data, CCTV footage, social media activity, emails, and online tracking. These tools are used to identify suspects, gather evidence, and prevent crime. While digital tools can While they make investigations faster and more efficient, they also give the police greater control over personal information. This raises serious concerns about privacy, abuse of power, and violation of fundamental rights. The Indian NSA Code, 2023 (BNSS)2 was enacted to replace the Code of Criminal Procedure, 1973.3 One of the key features of the BNSS is the formalization of digital methods of investigation and the recognition of electronic evidence. The law aims to modernize criminal procedure and adapt it to the needs of the present day. However, the expansion of digital policing powers raises important constitutional questions, particularly with regard to Article 21.

This research paper examines whether, within the framework of digital policing, the BNSS, 2023 protects the right to a fair investigation guaranteed under Article 21 of the Constitution. It studies the meaning and scope of fair investigation, digital tools in policing, and human rights concerns arising from technology-based investigations. The paper also analyzes whether the

ISSN: 2582-6433

BNSS provides adequate safeguards to prevent the misuse of digital powers.

Keywords: Right to a Fair Investigation, Article 21, Digital Policing, Electronic Evidence, Indian Civil Security Code 2023, Criminal Justice System, Privacy Rights, Constitutional Safeguards, Police Powers, Technology-Based Investigations, Due Process, Fundamental Rights, Digital Surveillance, Criminal Procedure Reforms

Chapter 1: Introduction

1.1 Meaning and Significance of Article 21

Article 21 of the Indian Constitution states that no person shall be deprived of his life or personal liberty except according to procedure established by law.4 At first glance, this provision appears simple. However, over the years, the Supreme Court has given Article 21 a much broader and meaningful interpretation. Initially, Article 21 was interpreted narrowly. As long as a law existed and procedure was followed, the courts did not question whether that procedure was fair or reasonable. This view changed after landmark judgments where the Court held that procedure must not only be legal but also fair, just, and reasonable.

Today, Article 21 encompasses several important rights such as the right to dignity, privacy, the right against arbitrary arrest, and the right to a fair trial. One of the most significant developments under Article 21 is the recognition of the right to a fair investigation.

1.2 Investigation as the Foundation of Criminal Justice

A criminal case begins with an investigation. The police gather evidence, question witnesses, and decide whether a person should be charged with a crime. This stage is extremely important because it determines the course of the entire case.

If the investigation is biased, careless, or dishonest, an innocent person may be falsely accused. On the other hand, a guilty person may escape punishment if evidence is suppressed or manipulated. Courts have repeatedly stated that justice cannot be achieved unless the investigation itself is fair.

The accused person is most vulnerable during the investigation phase. At this stage, the police have extensive powers, while the accused has limited protection. Therefore, constitutional protections during investigation become very important.

1.3 Evolution of the Right to a Fair Investigation

The concept of a fair investigation evolved through judicial decisions. The Supreme Court has

ISSN: 2582-6433

held in numerous cases that a fair investigation is part of the right to life and personal liberty under Article 21. The Court has stated that the police must act impartially and not with a fixed intent to prove guilt. Investigating officers are required to collect all relevant evidence, including evidence that may help the accused. Any investigation influenced by political pressure, personal interest, or bias violates Article 21.9. The courts have also held that if an investigation is unfair, higher courts can order a further investigation, reinvestigation, or investigation by an independent agency**.**

1.4 The Changing Nature of Policing in India

Traditional policing relied primarily on physical evidence, oral statements, and eyewitness evidence. However, modern society generates vast amounts of digital data. People use mobile phones, social media, email, and online platforms in their daily lives.

As a result, police investigations now rely heavily on digital data. Call records, GPS location, CCTV footage, and online activity are commonly used as evidence. Digital policing has become an essential part of law enforcement.

This shift has transformed the nature of investigations. Police can now monitor activities remotely and collect information without physical presence. While this helps crime control, it also increases the risk of surveillance without adequate controls.

1.5 The Need for Legal Regulation of Digital Policing

Digital tools are powerful. If used correctly, they can help deliver justice.

However, if used without regulation, they can violate fundamental rights. Microscope surveillance can impact privacy. Data can be misused, leaked, or manipulated. Without clear legal boundaries, digital investigations can become arbitrary. Therefore, it is important that criminal procedure laws clearly regulate how digital devices are used, how data is collected, and how individual rights are protected.

1.6 Introduction to the Indian Civil Protection Code, 2023

The Indian Civil Protection Code, 2023 was enacted to replace the Code of Criminal Procedure, 1973. The BNSS aims to modernize criminal procedure and remove outdated colonial provisions. One of the key features of the BNSS is the recognition of electronic evidence and digital procedures.11 The law allows the use of digital records and technology-based investigative methods. However, the BNSS also raises important constitutional questions. While it expands police powers in the digital space, it does not clearly state how misuse will

ISSN: 2582-6433

be prevented.

1.7 Research Problem

The main research problem addressed in this study is: whether the framework of digital policing under the Indian Civil Services Code, 2023, adequately protects the right to a fair investigation under Article 21 of the Constitution of India.

1.8 Objectives of the Study

The objectives of this research are: to understand the meaning and scope of fair investigation under Article 21; to study the concept and practice of digital policing in India; to analyze the provisions of the BNSS related to digital investigation; to examine human rights concerns arising from digital policing; and to suggest measures to ensure fairness and accountability.

1.9 Research Methodology

This research is theoretical in nature. It is based on the study of constitutional provisions, statutes, judicial decisions, and secondary sources such as books and articles. 24 Comparative references are also used where necessary.

Chapter 2: The Concept of Fair Investigation under Article 21

2.1 Meaning of Investigation

In criminal law, an investigation is the process by which the police collect facts and evidence related to a crime. It involves visiting the crime scene, questioning witnesses, collecting documents, seizing objects, and identifying suspects. The purpose of an investigation is to ascertain the truth and determine whether a crime has been committed and by whom. The investigation is the first and most important stage of the criminal justice process. If the investigation is shoddy or improper, the entire case is weakened. The courts depend largely on the investigation report prepared by the police. Therefore, the quality and fairness of the investigation directly impact justice.

2.2 The Concept of Fairness in Criminal Procedure

Fairness in criminal procedure means that the process must be just, reasonable, and impartial. This does not mean that the accused must always be acquitted. It means that the procedure used to determine guilt or innocence must be honest and lawful. The idea of fairness is deeply rooted in Article 21. The Supreme Court has held that any procedure affecting life or liberty must be

ISSN: 2582-6433

fair, just, and reasonable. This applies not only to trials but also to investigations.

2.3 Evolution of Article 21 and Due Process

In the early years after independence, Article 21 was interpreted narrowly. The courts adhered to a strict view that as long as law and procedure were followed, Article 21 was satisfied.12 This view changed after the landmark decision in Maneka Gandhi v. Union of India. The Supreme Court held that "procedure established by law" must be fair, just, and reasonable. Arbitrary or oppressive procedures violate Article 21.13 This decision laid the foundation for procedural due process in India. Following this case, courts began to examine not only whether a process existed, but also whether it was fair.

2.4 Judicial Recognition of a Fair Investigation

The Supreme Court has clearly stated in several cases that a fair investigation is a constitutional requirement under Article 21. The Court has stated that investigations must be free from bias, pressure, and influence.

In numerous cases, the Court has stated that police should not act with a preconceived mindset, and that investigating officers must collect all evidence, whether it supports the prosecution or the accused. Suppression of evidence is a serious violation of impartiality. The Court has also stated that if an investigation is unfair, it affects the credibility of the entire criminal justice system.

2.5 Investigations Must Be Impartial

Impartiality is the core of a fair investigation. The police should not favour one party over another. The investigation should not be influenced by political power, social pressure, or personal interest. If the investigating officer works only to prove the guilt of the accused and ignores evidence in favour of the accused, the investigation becomes unfair.

The courts have strongly criticized such conduct. An impartial investigation ensures public confidence in the justice system. It reassures citizens that the law treats everyone equally.

2.6 The Role of Courts in Ensuring Fair Investigations

Courts play a vital role in protecting the right to a fair investigation. When courts find that an investigation is biased or flawed, they have the power to intervene. Courts can order further investigation, direct reinvestigation, or transfer the investigation to an independent agency.15 These powers are exercised to protect Article 21 and prevent miscarriage of justice.

ISSN: 2582-6433

2.7 Fair Investigation and Rights of the Accused

During an investigation, the accused has certain basic rights. These include protection from illegal arrest, torture, and coercion. The accused also has the right to legal representation and to be informed of the grounds for arrest.16 A fair investigation respects these rights. Any investigation conducted in violation of these rights is unconstitutional. The Supreme Court has repeatedly held that the police cannot use illegal methods to extract confessions or evidence. Such practices violate Article 21.

2.8 Balance between Societal and Individual Rights

A fair investigation does not mean weakening the police. It means balancing the interests of society and individual liberty. Society has the right to be protected from crime.[26] At the same time, individuals have the right to dignity and liberty. A fair investigation maintains this balance by allowing a lawful investigation without the abuse of power.

2.9 Fair Investigation as a Continuous Process

Impartiality is not limited to one stage. It must be present throughout the investigation. From registration of the FIR to filing the charge sheet, impartiality must be maintained at every step.[27] Any delay, manipulation, or selective investigation affects impartiality. Courts have recognized that impartiality is a continuing obligation of the state.

2.10 Impact of Improper Investigation

Improper investigation can lead to the wrongful implication of innocent people, acquittal of guilty persons, loss of public confidence in the police, and violation of fundamental rights.
Due to these serious consequences, courts have considered fair investigation as a constitutional mandate.[28]

Chapter 3: Evolution of Criminal Procedure in India

3.1 Meaning of Criminal Procedure

Criminal procedure is a set of rules that govern how crimes are investigated, how offenders are prosecuted, and how courts conduct criminal trials. It defines the powers of the police, the rights of the accused, and the role of the courts. Criminal procedure is important because it controls the power of the state. Without due process, police powers can be abused, and individual liberty can be threatened. Therefore, criminal procedure laws must balance crime control with the protection of fundamental rights.

ISSN: 2582-6433

3.2 Criminal Procedure During the Colonial Period

During British rule, criminal laws in India were primarily designed to protect the interests of the colonial government. The criminal justice system was strict and granted broad powers to the police. The Code of Criminal Procedure was first introduced in the 19th century. Its primary purpose was to maintain order, not to protect individual rights. The system focused more on control than fairness. Many provisions permitted arrest, search, and detention with limited safeguards. Consideration of human rights or individual liberty was not a priority during this period.

3.3 Code of Criminal Procedure, 1898

The Code of Criminal Procedure, 1898 was a key colonial law that governed criminal procedure for several decades.29 It laid down detailed rules for investigation, trial, and punishment. Although the 1898 Code provided structure, it granted extensive discretion to the police. Safeguards for the accused were limited. Courts had little power to intervene during the investigation phase. This Code continued for some time after independence, demonstrating how deeply colonial thinking was embedded in Indian criminal law.

3.4 Changes in Criminal Procedure After Independence

After independence, India adopted the Constitution, which guaranteed fundamental rights. This required changes to criminal procedure to align with constitutional values. Courts began examining criminal procedure laws in light of Article 21. Gradually, the focus shifted from strict control to fairness and rationality. However, despite these constitutional developments, many colonial provisions remained in practice.

3.5 Code of Criminal Procedure, 1973

The Code of Criminal Procedure, 1973 replaced the Code of 1898. Modernizing criminal procedure and incorporating safeguards for the accused. The CrPC, 1973 introduced clear rules on arrest, the rights of the accused during investigation, greater judicial supervision, and provisions for legal aid. However, the CrPC was drafted at a time when digital technology did not exist. It focused primarily on physical evidence, paper records, and oral statements.

3.6 Judicial Interpretation of the CrPC and Article 21

Courts played a major role in reforming criminal procedure under the CrPC. Through judicial interpretation, courts added constitutional safeguards. Important developments included

ISSN: 2582-6433

prohibitions on arbitrary arrest, protection against torture in custody, the right to legal representation, and the right to a speedy trial. These safeguards were not always explicitly written in the CrPC but were read down through Article 21.

3.7 Limitations of the CrPC in the Digital Age

With the rise of digital technology, the CrPC began to show limitations. It did not clearly address electronic evidence, digital surveillance, or online data.32 Police began using digital tools based on practical necessity, but the law did not provide clear guidance. This created legal uncertainty and increased reliance on judicial interpretation. The absence of clear statutory rules has created confusion regarding privacy, consent, and digital evidence management.

3.8 Introduction to the Indian Civil Protection Code, 2023

The Indian Civil Services Code, 2023 was introduced to replace the CrPC, 1973. The BNSS aims to decolonize criminal law and modernize the process. The BNSS recognizes the use of electronic records, digital communications, and technology-based investigations. This reflects the reality that criminal investigations today rely heavily on technology.[17]

Chapter 4: Digital Policing: Meaning, Scope, and Practice in India

4.1 Meaning of Digital Policing

Digital policing refers to the use of technology and electronic devices by police to prevent crime, investigate crimes, and gather evidence. Instead of relying solely on physical evidence and eyewitnesses, police now use digital data. Digital policing includes the use of mobile phone records, CCTV footage, GPS tracking, email, social media activity, online transactions, and computer data. These tools help police understand incidents and identify suspects.

4.2 The Development of Technology in Daily Life

Technology has become a part of everyday life. People communicate through mobile phones, messaging apps, and social media. Payments are made online. Locations can be tracked using GPS. Because of this, crimes are also planned, committed, and reported using digital platforms. This has forced the police to adopt digital methods. Traditional investigation methods alone are no longer sufficient to tackle modern crimes such as cyber fraud, online harassment, and digital financial crimes.

ISSN: 2582-6433

4.3 Common Digital Tools Used by Police

Police use various digital tools during investigations. Some of the most common tools include call detail records (CDRs), which show who called whom, when, and from where; CCTV footage; mobile phone data, including messages and logs; youth tracking; media monitoring; facial recognition systems; and GPS tracking. These tools help police gather evidence faster and more efficiently.

4.4 Digital Policing and Privacy Concerns

Digital policing directly impacts the right to privacy. Personal data such as messages, photos, location, and online activity can be accessed during investigations. Without clear regulations, digital surveillance can become excessive. There is a risk of collecting more data than necessary. The Supreme Court has recognized privacy as a fundamental right. Article 21.[18] Therefore, digital policing must respect privacy boundaries.

4.5 Risk of Misuse of Digital Powers

Digital tools give police broad powers. If these powers are misused, they can harm innocent people. Data can be selectively used or misinterpreted. There is also a risk of false implications based on digital records.[34] Without proper training and accountability, digital policing can become a tool of oppression.

4.6 Need for Regulation of Digital Policing

Digital policing is necessary, but it must be regulated. Clear legal rules are needed to regulate how digital devices are used. The rules should explain when surveillance can be used, how long data can be stored, who can access the data, and the extent of misuse. Regulation is necessary to protect 35 fundamental rights.

Chapter 5: The Indian Civil Security Code, 2023: Digital Investigation and Electronic Evidence

5.1 Introduction to the BNSS, 2023

The Indian Civil Security Code, 2023 was enacted to replace the Code of Criminal Procedure, 1973. The objective of introducing the BNSS was to modernize criminal procedure and remove colonial influences from Indian criminal laws. One of the most important features of the BNSS is the recognition of technology in criminal investigations. The law acknowledges that digital

ISSN: 2582-6433

evidence and electronic procedures are now a routine part of policing.

5.2 Recognition of Electronic Records

The BNSS recognizes electronic records as a valid form of evidence. This includes emails, messages, digital documents, CCTV footage, call records, and other electronic [19] Under earlier laws, electronic evidence was often dealt with indirectly. Now, the BNSS explicitly permits the use of such material during investigations and trials. This recognition reflects the reality that many crimes involve digital communication and online activity.

5.3 Use of Technology in Investigations

The BNSS allows police to use technology for investigation-related activities. This includes recording statements, collecting electronic data, and maintaining digital records.36 The law encourages the use of technology to improve efficiency and reduce delays. Digital methods are considered faster and more reliable than traditional paper-based systems. However, the BNSS does not always explain the exact limitations of the use of such technology.

5.4 Seizure of Electronic Devices

The BNSS allows police to seize electronic devices during investigations. This may include mobile phones, laptops, tablets, and storage devices.37 Such seizures can seriously impact personal lives, as these devices contain private information. Therefore, seizures must be carried out carefully and legally. The BNSS does not provide detailed information on how seized devices should be handled or returned, or on security measures, which may affect personal freedom.

5.5 Storage and Preservation of Digital Evidence

Digital evidence must be properly stored to maintain its authenticity. If data is not properly preserved, it may lose its value as evidence. BNSS recognizes the importance of preserving electronic records but does not maintain uniform technical standards.38 This lack of clarity can lead to different practices across states and agencies, affecting fairness.

5.6 Chain of Custody of Electronic Evidence

Chain of custody means a record of who handled the evidence and when. This is critical to prove that the evidence was not tampered with. In the case of digital evidence, maintaining the chain of custody is more complex. Data can be copied, altered, or deleted.[39] BNSS does not

ISSN: 2582-6433

provide detailed rules for maintaining the chain of custody of electronic evidence, which may raise doubts about its reliability.

5.7 Use of CCTV and Surveillance Data

BNSS allows the use of CCTV footage and surveillance data as evidence. Such footage is typically used to track activities and identify suspects. While CCTV evidence can be helpful, it also raises privacy concerns.40 Continuous surveillance of public and private spaces can impact freedom. BNSS does not clearly state how the misuse of surveillance data will be prevented.

Chapter 6: Human Rights Implications of Digital Policing under BNSS

6.1 Right to Privacy under Article 21

The right to privacy is recognized as a fundamental right under Article 21. Privacy includes personal choices, communications, movements, and personal data.20 Digital policing involves accessing messages, call records, location data, and online activity. Such access directly impacts privacy. If surveillance and data collection are not properly controlled, they can lead to unnecessary intrusion into private life.

6.2 Mass Surveillance and Its Impact

Digital devices allow mass surveillance. CCTV cameras, online monitoring, and tracking systems can constantly monitor people. Mass surveillance treats everyone as a potential suspect. This goes against the principle that investigations should be based on reasonable suspicion.41 Continuous surveillance can impact freedom of expression and movement, which are closely linked to personal liberty.

6.3 Risk of Bias and Discrimination

Digital policing tools often rely on existing data. If past policing practices were biased, digital tools may replicate those biases. Certain communities may be more monitored based on location, social background, or online behavior.42 Selective surveillance violates the principle of equality and fairness.

6.4 Right against self-incrimination

Digital investigations sometimes involve extracting data from personal devices. This can indirectly compel a person to give evidence against themselves. The right against self-

ISSN: 2582-6433

incrimination is a fundamental legal protection.21 Digital methods must respect this right. Ambiguous rules on data extraction raise serious constitutional concerns.

6.5 Due Process and Fair Trial Concerns

A fair investigation is closely linked to the right to a fair trial. If digital evidence is not properly shared with the defense, fairness is affected. Delays in providing access to digital records and a lack of technical explanations weaken the defense.[43] Due Process It is essential that the accused has a meaningful opportunity to challenge the evidence.

6.6 Lack of Strong Oversight Mechanisms

Oversight means supervision of police powers by independent authorities. In digital policing, oversight is weak. Most decisions regarding surveillance and data use are made[44] Without independent review, abuse of power becomes more likely.

Chapter 7: Challenges in Maintaining Objectivity Digital Investigations

7.1 Technical Complexity of Digital Evidence

Digital evidence is not as simple as physical evidence. It consists of data files, metadata, logs, and system records. Most people, including accused persons, lawyers, and even judges, may not fully understand how digital evidence works. Because of this complexity, it becomes difficult to verify whether evidence is genuine or manipulated.

7.2 Risk of Evidence Tampering

Digital data can be easily altered. A file can be edited, copied, or deleted without leaving visible traces. If proper security measures are not followed, there is a risk that digital evidence could be intentionally or accidentally altered.45 Maintaining objectivity requires strict protection against tampering, but such protection is often weak in practice.

7.3 Problems with Chain of Custody

Chain of custody means identifying who handled evidence, when, and how. In digital investigations, evidence passes through many hands—police officers, forensic experts, and technical staff.46 If records are not properly maintained, the reliability of evidence becomes questionable.

ISSN: 2582-6433

7.4 Lack of Technical Training Among Police

Many investigating officers do not receive proper training in digital forensics. Without technical knowledge, officers may make mistakes during the seizure, storage, or analysis of equipment.47 Such mistakes can damage evidence and even affect the rights of the accused.

7.5 Lack of Uniform Standards

Different states follow different procedures for digital investigations. There is no single national standard for handling electronic evidence.48 This lack of uniformity leads to inconsistency and uncertainty in criminal investigations.

7.6 Access to Digital Evidence for the Defense

Fair investigations require that the accused have access to the evidence against them. In digital cases, access is often delayed or restricted due to technical reasons.49 Without full access, the defense cannot properly challenge the prosecution's case.

Chapter 8: Comparative Insights on Digital Policing and Fair Investigations

8.1 United Kingdom

The United Kingdom uses digital tools such as CCTV surveillance, data analysis, and electronic evidence in investigations. However, digital policing is governed by a strict legal framework. Surveillance powers require authorization and are subject to review.50 Independent bodies monitor police conduct. Courts closely examine whether digital evidence was collected legally. This system shows that technology can be used while respecting individual rights.

8.2 United States

In the United States, digital evidence is widely used in criminal cases. The Constitution protects privacy through safeguards against unreasonable searches. Access to personal data often requires a warrant.[22] Courts actively review digital searches to ensure they do not infringe on personal liberty. This approach highlights the importance of judicial oversight in digital investigations.

8.3 European Union

The European Union emphasizes data security and privacy. Strict regulations govern data collection, storage, and use.51 Individuals have rights over their personal data. Law enforcement agencies must follow clear legal procedures when using digital tools. This model

ISSN: 2582-6433

focuses on transparency and accountability.

8.4 Lessons for India

Comparative analysis shows that democratic countries do not allow unrestricted digital policing. Key general principles include legal authority for surveillance, strong judicial oversight, independent monitoring bodies, clear data protection rules, and transparency in evidence management. India can adopt these principles while implementing the BNSS.

Chapter 9: Evaluating the BNSS, 2023 through the lens of Article 21

9.1 Introduction

The Indian Civil Services Code, 2023 was introduced to modernize criminal proceedings in India. One of its key objectives is to use technology to make investigations faster and more efficient. However, any procedural law must comply with Article 21 of the Constitution. Article 21 does not merely permit lawful procedure; it requires fair, just, and reasonable procedure.

9.2 Lack of Detailed Safeguards

The BNSS does not provide detailed rules for data collection limits, storage periods, access control, or destruction of irrelevant data. This creates uncertainty and scope for misuse.53 Such gaps raise concerns under Article 21.

9.3 Discretionary Powers of the Police

Digital investigation powers under the BNSS grant police officers broad discretion. Without strict scrutiny, discretionary powers can be abused. Article 21 requires limits on state power to prevent arbitrariness.[23]

9.4 Issues of Consent and Coercion

The BNSS does not clearly state how consent should be obtained to access digital devices. In practice, consent may be obtained under duress.[54] Vague consent rules weaken personal liberty protections.

9.5 Right to Privacy Concerns

Digital policing involves access to personal data and communications. The BNSS does not fully integrate privacy safeguards. Privacy intrusions without proportionality violate Article 21.[55]

ISSN: 2582-6433

9.6 Limited Judicial Oversight

Judicial oversight is essential to control investigative powers. The BNSS does not Mandate judicial approval for all forms of digital surveillance.56 Limited oversight Reduces accountability and increases the risk of rights violations.

9.7 Conclusion

While the BNSS 2023 modernizes criminal procedure and recognizes digital investigation, it fails to provide adequate constitutional safeguards. The absence of detailed protections for privacy, consent, oversight, and defense rights raises serious concerns under Article 21. To make digital policing truly constitutional, the law must balance efficiency with fundamental rights through clear boundaries, strong oversight, and transparent procedures.[57]

Chapter 10: Recommendations for Fair and Rights- Based Digital Policing

10.1 Introduction

Digital policing is now an indispensable part of criminal investigations. Technology can help solve crimes quickly and accurately. However, without proper regulations, it can also harm individual freedoms. To ensure that digital investigations under the BNSS remain fair and constitutional, strong safeguards are needed. This chapter suggests practical recommendations to protect Article 21 rights when using technology.

10.2 Establish a Clear Legal Framework

The BNSS should include detailed rules for digital investigations. These rules should clearly explain:

- When digital devices can be used
- What data can be collected
- How long data can be stored
- When data must be deleted

Clear rules reduce abuse and confusion.

10.3 Judicial Authorization for Surveillance

Digital surveillance should require prior approval from a judicial authority. Judicial authorization ensures that surveillance is necessary and proportionate. This protects individuals from arbitrary state action.

ISSN: 2582-6433

10.4 Strong Consent Standard

Consent to access digital devices must be:

- Voluntary
- Informed
- Recorded in written or digital form

The accused must understand the consequences of giving consent. This strengthens the protection of personal liberty.

10.5 Independent Oversight Body

An independent body should monitor police use of digital tools.

This body can:

- Review surveillance practices
- Investigate complaints
- Ensure compliance with legal standards

Oversight improves accountability and trust.

10.6 Uniform National Standards

There should be uniform standards for digital evidence across India. Standardized procedures ensure consistency and fairness. They also help courts evaluate evidence more effectively.

10.7 Capacity Building and Training

Police officers should receive appropriate training in digital forensics. Training should include:

- Technical skills
- Legal safeguards
- Human rights principles

Well-trained officers reduce errors and rights violations.

10.8 Transparency in Digital Investigations

Officers should maintain transparency in how they use digital tools. Clear documentation of digital procedures helps courts and defence lawyers. Transparency strengthens procedural fairness.

ISSN: 2582-6433

10.9 Access to Digital Evidence for the Defence

Accused should have timely and full access to digital evidence. This includes copies of electronic records and forensic reports. Access ensures an effective defence and fair trials.

10.10 Data Security Measures

Strong data protection rules should be introduced. These should be prevented:

- Unauthorized access
- Data leaks
- Misuse of personal information

Data security supports the right to privacy.

10.11 Limiting surveillance to serious crimes

Digital surveillance should be limited to serious crimes. This prevents unnecessary intrusion into private life. Proportionality is required under Article 21.

10.12 Regular audits of digital devices

Digital policing tools should be regularly audited. Audits ensure that the tools are accurate and fair. This reduces the risk of wrongful targeting.

10.13 Public awareness and legal literacy

People should be informed about their digital rights. Legal awareness helps citizens protect themselves from misuse. An informed public strengthens democracy.

10.14 The role of courts in protecting rights

Courts should actively scrutinize digital investigation methods. Judicial investigations ensure constitutional compliance. Courts should not blindly accept digital evidence.

10.15 Balancing Technology and Humanity

Technology should assist, not replace, human judgment. Investigations must remain sensitive to human dignity. Justice must always remain people-centered.

10.16 Conclusion of the Chapter

These recommendations aim to strengthen fairness in digital policing. By adopting rights-based safeguards, the BNSS can align with Article 21. Effective investigations and the protection of

ISSN: 2582-6433

human rights must go hand in hand. The final chapter will present the overall conclusions of the study.

Chapter 11: Conclusion

11.1 Introduction

The criminal justice system in India is undergoing a major transformation. The use of technology in investigations is rapidly increasing. The Indian Civil Defence Code, 2023 reflects this change by formally recognizing digital methods and electronic testimony.

However, modernization of the law must always respect the Constitution. Article 21 is at the heart of individual liberty and fair process. This study examined whether digital policing under the BNSS supports or threatens the right to a fair trial under Article 21.

11.2 Importance of Fair Investigation

A fair investigation is the foundation of a fair trial. Without fairness at the investigative stage, justice cannot be achieved.

The Supreme Court has repeatedly stated that investigations must be honest, impartial, and free from arbitrariness. These principles apply equally to traditional and digital investigations. Technology cannot be allowed to undermine these constitutional protections.

11.3 Digital Policing: Opportunities and Risks

Digital policing offers many advantages. It facilitates faster evidence collection, better documentation, and improved crime detection. Electronic records, CCTV footage, and digital communications can strengthen investigations when used responsibly. At the same time, digital tools pose serious risks. Surveillance, data collection, and device use directly impact privacy and personal liberty.

11.4 BNSS and Its Constitutional Impact

BNSS takes a progressive step by acknowledging modern investigative realities. It updates criminal procedure to match technological developments. However, the law does not provide detailed safeguards for digital investigations. Crucial issues such as consent, data protection, surveillance limits, and oversight are not clearly addressed.

This creates a gap between efficiency and constitutional fairness.

ISSN: 2582-6433

11.5 Article 21 as a Limiting Force

Article 21 serves as a safeguard against the abuse of state power. This requires that all procedures must be fair, just, and reasonable. Any digital investigation method that is arbitrary or excessive violates Article 21. Therefore, digital policing under the BNSS must be interpreted and implemented in a rights-protective manner.

11.6 Human Rights Concerns

This study highlighted several human rights concerns:

- Privacy invasion
- Risk of misuse of digital evidence
- Bias and discrimination
- Weak access to defence
- Lack of independent oversight

Without addressing these concerns, digital policing could damage public trust and democracy.

11.7 The Need for Strong Safeguards

Technology alone cannot deliver justice. Legal safeguards, accountability, and transparency are equally important. Judicial oversight, clear procedures, officer training, and data protection rules are essential to maintain impartiality. The recommendations in this study aim to strengthen these safeguards.

11.8 Role of the Judiciary and Legislature

Courts have a crucial role in protecting Article 21. Judicial scrutiny of digital evidence is essential to prevent injustice. Additionally, the legislature must update laws to clearly regulate digital policing. A concerted effort is needed to ensure constitutional compliance.

11.9 The Future of Digital Policing in India

Digital policing is not temporary. It will continue to expand with technology. The challenge is not whether to use technology, but how to use it responsibly. India must develop a rights- based digital investigation framework that respects dignity and freedom.

11.10 Final Observations

This research concludes that:

ISSN: 2582-6433

- Digital policing can improve investigations
- But without safeguards, it may violate Article 21. BNSS is a step forward, but incomplete
- Constitutional values should guide technology use
- A fair investigation is not an obstacle to justice. It is the path to justice.

11.11 Concluding Notes

The legitimacy of the criminal justice system depends on public trust. That trust is built when investigations are fair, transparent, and constitutional. Digital policing should serve justice, not control citizens. Only when efficiency is balanced with human rights can the promise of Article 21 be truly fulfilled.

Chapter 12: Empirical Study (Survey Analysis with numerical percentages)

12.1 Introduction

This chapter is based on a survey conducted by the researcher to understand public awareness and opinions about digital policing, BNSS, 2023, and fair investigation under Article 21.
A total of 40 respondents participated in the survey.

12.2 Respondent Profile

- Age group 18-25 years: 34 respondents (85%)
- Age group 26-35 years: 4 respondents (10%)
- Age group 36-50 years: 2 respondents (5%)

Occupancy:

- Students: 34 respondents (85%)
- Academic/Research: 4 respondents (10%)
- Government/Private Sector: 2 respondents (5%)

12.3 Question-wise Analysis

Question 1: Awareness about the Indian Criminal Justice System

- Well informed: 22 respondents (55%)
- Somewhat aware: 12 respondents (30%)
- Not aware: 6 respondents (15%)

ISSN: 2582-6433

Explanation:

More than half of respondents are well-informed about the criminal justice system.

Question 2: Have you studied anything related to law, policing, or human rights?

- Yes: 26 respondents (65%)
- Partially: 8 respondents (20%)
- No: 6 respondents (15%)

Explanation:

Most respondents have academic experience in legal or human rights topics.

Question 3: Awareness about BNSS, 2023

- Yes, fully aware: 19 respondents (47.5%)
- Somewhat aware: 16 respondents (40%)
- Not aware: 5 respondents (12.5%)

Explanation:

Most respondents are aware of BNSS, although their full understanding is limited.

Question 4: Knowledge of the difference between the BNSS and the CrPC

- Yes: 14 respondents (35%)
- Partially: 16 respondents (40%)
- No: 10 respondents (25%)

Explanation:

While awareness exists, detailed legal knowledge is still developing.

Question 5: Awareness that the BNSS promotes digital methods in investigations

- Yes: 26 respondents (65%)
- Partially: 8 respondents (20%)
- No: 6 respondents (15%)

Explanation:

Digital investigations are widely recognized under the BNSS.

Question 6: Awareness of electronic evidence provisions under the BNSS

- Yes: 22 respondents (55%)

 ISSN: 2582-6433

- Not sure: 10 respondents (25%)
- No: 8 respondents (20%)

Explanation:

More than half of respondents are aware of e-evidence, but lack clarity.

Question 7: Does digital policing improve investigation accuracy?

- Agree/strongly agree: 28 respondents (70%)
- Neutral: 8 respondents (20%)
- Disagree: 4 respondents (10%)

Explanation:

A strong majority believe that technology improves investigation accuracy.

Question 8: Concerns about police access to personal digital data

- Very concerned: 22 respondents (55%)
- Somewhat concerned: 12 respondents (30%)
- Not concerned: 6 respondents (15%)

Explanation:

Privacy is a major concern among respondents.

Question 9: Can digital evidence be tampered with?

- Yes: 30 respondents (75%)
- No: 6 respondents (15%)
- Not sure: 4 respondents (10%)

Explanation:

Most respondents believe that digital evidence is vulnerable to manipulation.

Question 10: Are the safeguards under the BNSS sufficient to protect human rights?

- Yes: 10 respondents (25%)
- No: 18 respondents (45%)
- Not sure: 12 respondents (30%)

Explanation:

A large majority believe that the safeguards under the BNSS are inadequate.

ISSN: 2582-6433

Question 11: Should citizens' consent be required before accessing digital data?

- Yes: 32 respondents (80%)
- No: 4 respondents (10%)
- Depends on the case: 4 respondents (10%)

Explanation:

There is strong support for consent-based digital access.

12.4 Key Findings (with Percentage Summary)

- 65% of respondents support digital policing
- 55% are seriously concerned about privacy
- 75% believe that digital evidence can be tampered with
- 80% support consent before digital data access
- 45% feel that BNSS security measures are not adequate

12.5 Survey Findings

The survey clearly shows that while digital policing is widely accepted, privacy, fairness, and security measures remain serious concerns. The findings strongly support the need for constitutional protection under Article 21 in digital investigations.

BNSS. Footnotes

1. India Constitution Art. 21.
2. The Indian Civil Security Code, 2023, No. 46, Act of Parliament, 2023 (India).
3. Code of Criminal Procedure, 1973, No. 2, Act of Parliament, 1974 (India).
4. India Constable Art. 21.
5. Maneka Gandhi v. Union of India, (1978) 1 SCC 248 (India).
6. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).
7. D.K. Basu v. State of West Bengal, (1997) 1 SCC 416 (India).
8. Hussainara Khatoon v. Home Secretary, State of Bihar, (1979) AIR 1360 (India).
9. Babubhai v. State of Gujarat, (2010) 12 SCC 254 (India).
10. Zahira Habibullah Shaikh v. State of Gujarat, (2004) 4 SCC 158 (India).
11. Indian Civil Defence Code, 2023, §§ 94, 105, No. 46, Act of Parliament, 2023 (India).
12. A.K. Gopalan v. State of Madras, (1950) AIR 27 (India).
13. Maneka Gandhi v. Union of India, (1978) 1 SCC 248 (India).

ISSN: 2582-6433

14. Nirmal Singh Kahlon v. State of Punjab, (2009) 1 SCC 441 (India).
15. Com. for Protection of Democratic Rights v. State of West Bengal, (2010) 3 SCC 571 (India).
16. India Constitution Art. 22.
17. Indian Civil Security Code, 2023, Statement of Objects and Reasons, No. 46, Act of Parliament, 2023 (India).
18. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).
19. Indian Civil Security Code, 2023, § 2(1)(d) (definition of electronic communication).
20. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).
21. India Constitution Art. 20(3); Selvi v. State of Karnataka, (2010) 7 SCC 263 (India).
22. US Constitution Amendment IV; Katz v. United States, 389 US 347 (1967).
23. Maneka Gandhi v. Union of India, (1978) 1 SCC 248 (India).
24. S.N. Jain, Theoretical and Non-Theoretical Legal Research 15-28 (Deep & Deep Publications 2009).
25. Maneka Gandhi v. Union of India, (1978) 1 SCC 248, ¶ 5 (India).
26. State of Maharashtra v. Suresh, (2000) 1 SCC 471 (India).
27. Vineet Narain v. Union of India, (1998) 1 SCC 226 (India).
28. Rubabuddin Shaikh v. State of Gujarat, (2010) 2 SCC 200 (India).
29. Code of Criminal Procedure, 1898, Act No. 5 of 1898 (India) (repealed 1974).
30. Code of Criminal Procedure, 1973, Statement of Objects and Reasons, No. 2, Act of Parliament, 1974 (India).
31. D.K. Basu v. State of West Bengal, (1997) 1 SCC 416 (India) (establishing safeguards in custody).
32. Anwar P.V. v. P.K. Bashir, (2014) 10 SCC 473 (India) (highlighting gaps in electronic evidence procedures).
33. See generally Roger Clark, Surveillance Technologies and Their Implications Privacy (2019).
34. State of Punjab v. Baldev Singh, (1999) 6 SCC 172 (India).
35. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, ¶¶ 180-185 (India) (emphasizing the need for a data protection framework)
36. The Indian Civil Security Code, 2023, §§ 173, 176, No. 46, Act of Parliament, 2023 (India).
37. The Indian Civil Security Code, 2023, § 105, No. 46, Act of Parliament, 2023 (India).
38. The Information Technology Act, 2000, § 65B, No. 21, Act of Parliament, 2000 (India).

ISSN: 2582-6433

39. Tommaso Bruno v. State of Uttar Pradesh, (2015) 7 SCC 178 (India).
40. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, ¶ 127 (India) (discussing surveillance and privacy)
41. People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (India).
42. See Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (2018).
43. Zahira Habibullah Shaikh v. State of Gujarat, (2004) 4 SCC 158 (India).
44. See Law Commission of India, Report No. 260, Code of Criminal Procedure, 1973 (2015).
45. State (National Capital Territory of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600 (India).
46. Anwar P.V. v. P.K. Bashir, (2014) 10 SCC 473, ¶ 24 (India).
47. Bureau of Police Research and Development, Digital Forensics in Indian Policing: Challenges and Opportunities (2020).
48. See generally Ministry of Home Affairs, Model Police Act, 2006 (Government of India 2006).
49. Zahira Habibullah Shaikh v. State of Gujarat, (2004) 4 SCC 158, ¶¶ 38 (India).
50. Regulation of Investigatory Powers Act 2000, c. 23 (UK).
51. General Data Protection Regulation (GDPR), 2016/679, 2016 OJ (L 119) (EU).
52. See generally David Cole and Jules Lobel, Less Safe, Less Free: Why America is Losing the War on Terror (2007).
53. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, ¶¶ 180-188 (India) (emphasizing the need for clear statutory safeguards).
54. State of Uttar Pradesh v. Singhara Singh, (1964) 4 SCR 485 (India) (discussing voluntary consent).
55. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, ¶¶ 149-152 (India) (proportionality test for privacy intrusion).
56. People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301, ¶¶ 20 (India) (emphasizing judicial oversight for surveillance).
57. See generally Lawrence Lessig, The Code: Version 2.0 (2006) (discussing regulation of technology and individual rights).

ISSN: 2582-6433

Bibliography

Books and Textbook-Level Sources

Electronic Evidence - Nayan Joshi - A comprehensive book on digital/electronic evidence and forensics. Modern Indian criminal law, including BNSS and related statutes.

Electronic Evidence (Lawman, 2nd Edition, 2025) - https://www.priyalawhouse.com/product/31871320/Electronic-Evidence--Nayan-Joshi--2nd-Edn- 2025--

Lawman

Insights into Indian Criminal Law: Principles, Procedures, and Practice - General textbook covering Basics of criminal law, procedure, and investigation.

Insights into Indian Criminal Law: Principles, Procedures and Practice (PDF) – https://cpur.in/library/Books/56%20Insights%20into%20Indian%20Criminal%20Law.pdf

Right to a Fair Trial – National Judicial Academy Handout – Supports concepts related to fair trial and criminal procedure.

Right to a Fair Trial under the Indian Constitution (NJA PDF) – https://nja.gov.in/Concluded_Programmes/2019-20/P-1163_PPTs/1.Right%20to%20Fair%20Trial_Handout.pdf Journal Articles and Research Papers

Algorithmic Policing and Due Process in Cybercrime Investigations – A scholarly article analyzing digital policing, AI tools, and constitutional implications under Articles 14, 19, and 21.

Algorithmic Policing and Due Process – https://shodhsamajik.com/shodhsamajik/article/view/57From FIRs to Forensic Analysis in the Digital Age – Articles on Cybercrime Investigations, Digital Evidence, and Judicial Oversight under Indian Law (CrPC/BNSS/BSA).

From FIRs to Forensic Analysis – https://ijrdo.org/index.php/lcc/article/view/6300

Digital Evidence under the Indian Legal System – Problems and Perspectives – Explores digital evidence Challenges, admissibility, and evidentiary standards in India.

Digital Evidence under the Indian Legal System – https://www.jneonatalsurg.com/index.php/jns/article/view/9809

Legal/Constitutional Sources

Article 21 of the Constitution of India – Constitutional text and commentary on the right to life and personal liberty (with procedural fairness implications).

Article 21 – Indian Kanoon – https://indiankanoon.org/doc/1199182/ Other Scholarly/Relevant

ISSN: 2582-6433

Sources

Judicial Approaches to Predictive Policing and Electronic Surveillance in India – Paper on Police Surveillance, Privacy, and Constitutional Rights in India.

Predictive Policing and Surveillance Article - https://www.whiteblacklegal.co.in/details/judicial- approach

Police Surveillance in India - Bikram Singh - Issues related to the right to privacy in relation to police surveillance and electronic surveillance

Goraya

Cybercrime and Computer Forensics in India in the Age of Artificial Intelligence - Research on Digital Evidence, AI Risks, and Forensic Issues (Relevant References for Digital Investigation Challenges).

Cybercrime and Computer Forensics in India - https://arxiv.org/abs/2512.15799

Supplementary Material (Policy/Practice References)

Fair Investigation and Fair Trial - Police Journal Paper - Highlights why fair investigation is a constitutional requirement in India.

Fair Investigation: The Backbone of Criminal Justice - https://haryanapolice.gov.in/policejournal/pdf/fair_investigation.pdf